

Product name	Confidentiality level
mToken CryptoID	
Product version	
V1.1	

mToken CryptoID

Smart Card Application Guide

Prepared by		Date	
Reviewed by		Date	
Approved by		Date	



Century Longmai Technology Co., Ltd.

All rights reserved

Revision Record

Date	Revision Version	Sec No.	Change Description	Author
2015/1/23	V1.0		Initial Version	Longmai ITD

Contents

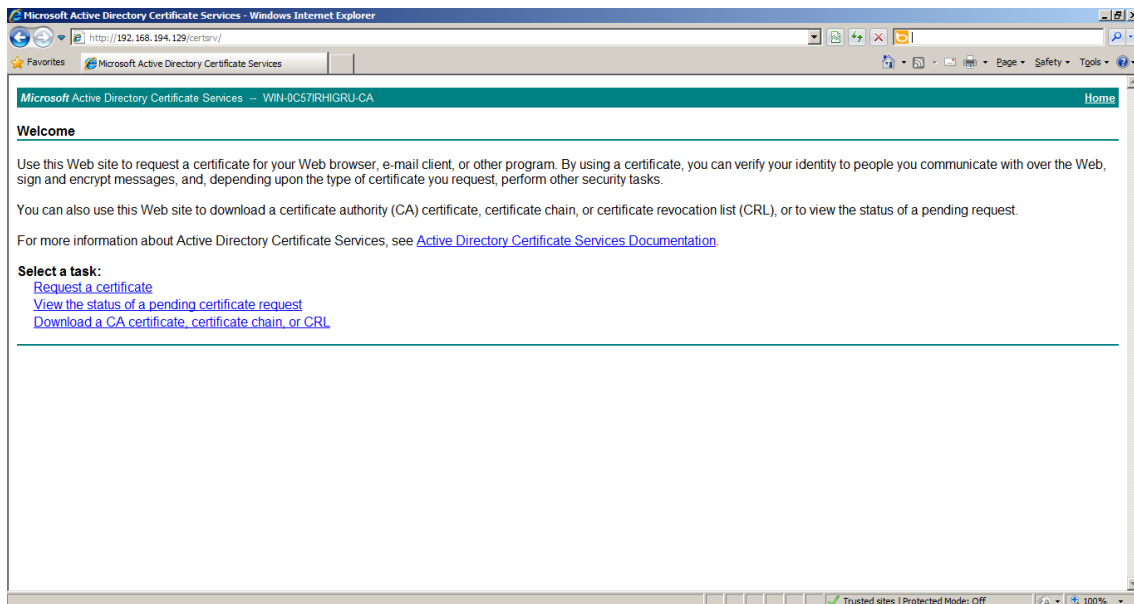
CHAPTER 1. SMART CARD LOGON.....	4
1.1 PREREQUISITES – REQUEST FOR SMART CARD LOGON CERTIFICATE	4
1.2 SMART CARD LOGON	7
CHAPTER 2. BITLOCKER DRIVE ENCRYPTION.....	20
2.1 REQUEST A BITLOCKER CERTIFICATE	20
2.2 DRIVE ENCRYPTION	22
CHAPTER 3. VPN.....	29
3.1 SERVER CONFIGURATION	29
3.1.1 VPN Installation	29
3.1.2 VPN Configuration	31
3.2 CLIENT CONFIGURATION	34
3.2.1 Request a Smart Card Logon Certificate	34
3.2.2 Establish Connection	36

Chapter 1. Smart Card Logon

From Microsoft Windows 2000 and above, MS included in-built smart card logon verification; the system user can either use traditional “username + password” to verify domain user or use smart card to automatically verify user identity. Comparing the two methods, smart card logon can be much safer and easy-to-use since the user is only needs to remember PIN of his/her smart card being used to logon.

1.1 Prerequisites – Request for Smart Card Logon Certificate

1. Make sure the mToken device has been connected to your computer.
2. Open the certificate server page through Internet Explorer. (Here I will access my CA Server at <http://192.168.194.129/certsrv/>)



3. Select **Request a certificate** → **Advanced Certificate Request** → **Create and submit an application to the CA.**
4. In Certificate Template Area, select smart card related template (Smartcard User or Smartcard Logon).
5. Select **Microsoft Base Smart Card Crypto Provider** as the CSP.

Certificate Template:

Smartcard Logon

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: Microsoft Base Smart Card Crypto Provider

Key Usage: ☒ Exchange

Key Size: 1024 Min:1024 Max:2048 (common key sizes: [1024](#) [2048](#))

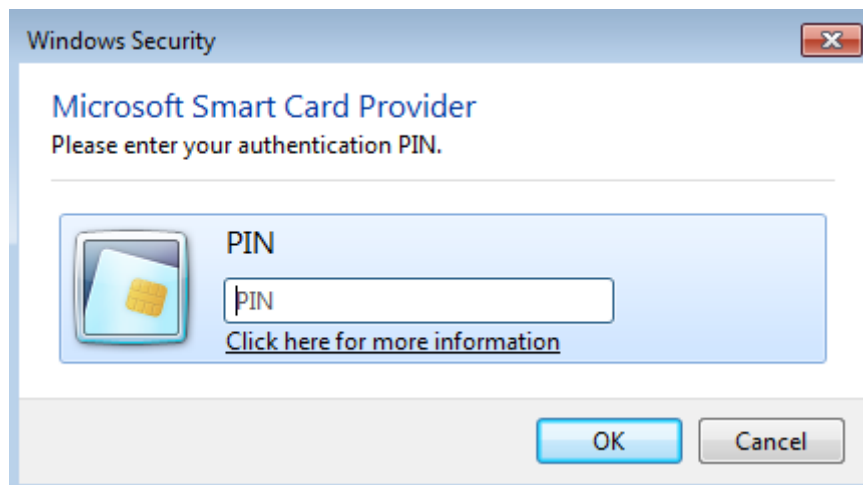
☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

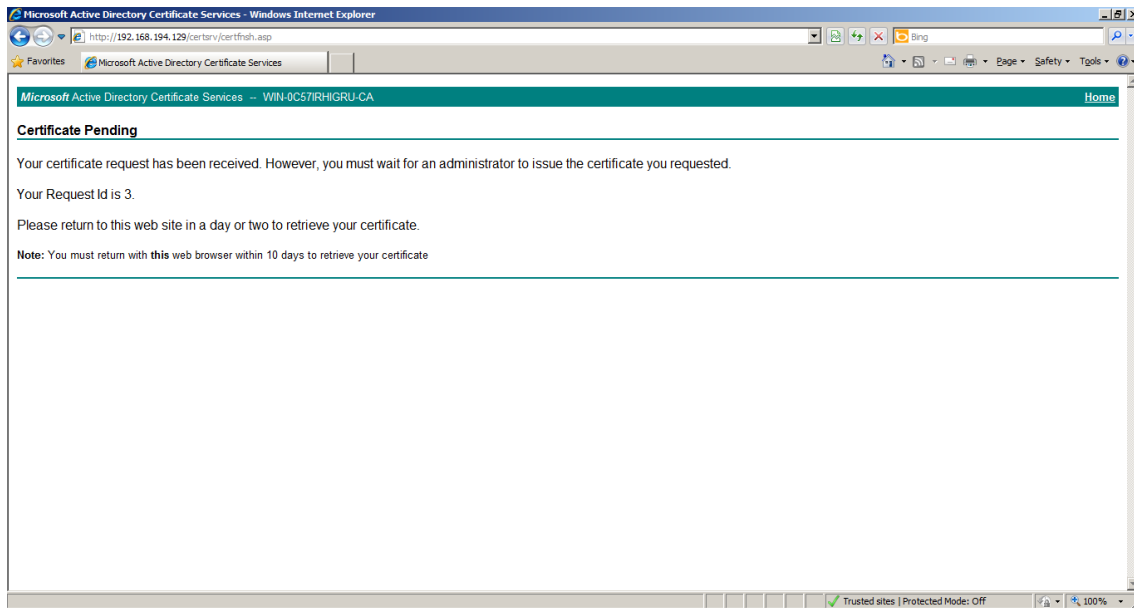
☐ Enable strong private key protection

Additional Options:

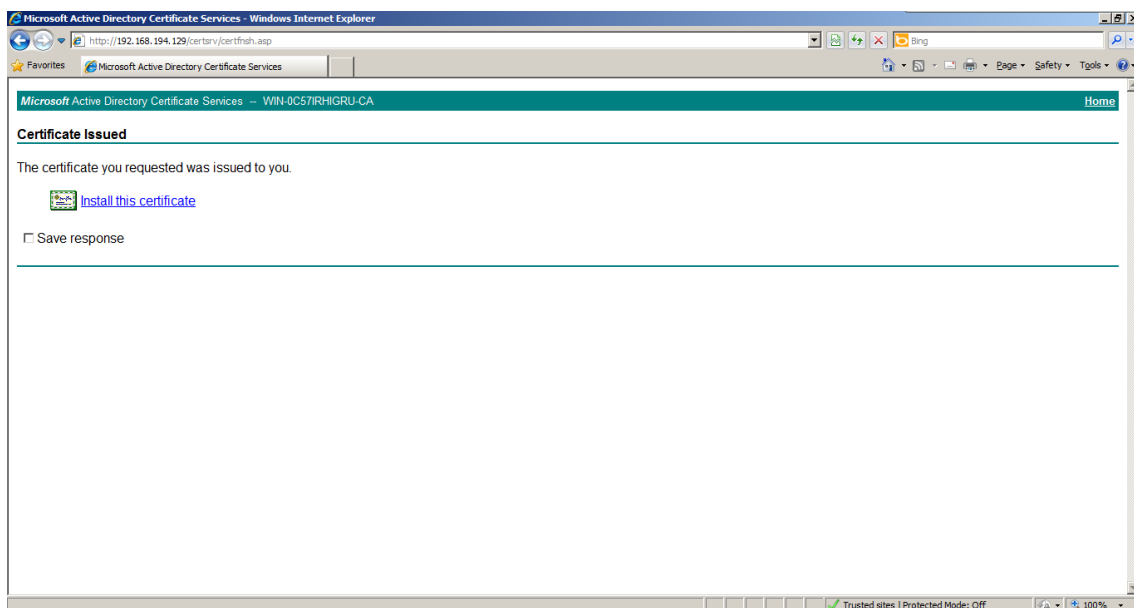
6. Finish the above Settings; click **Submit**, the PIN dialog box pops up.

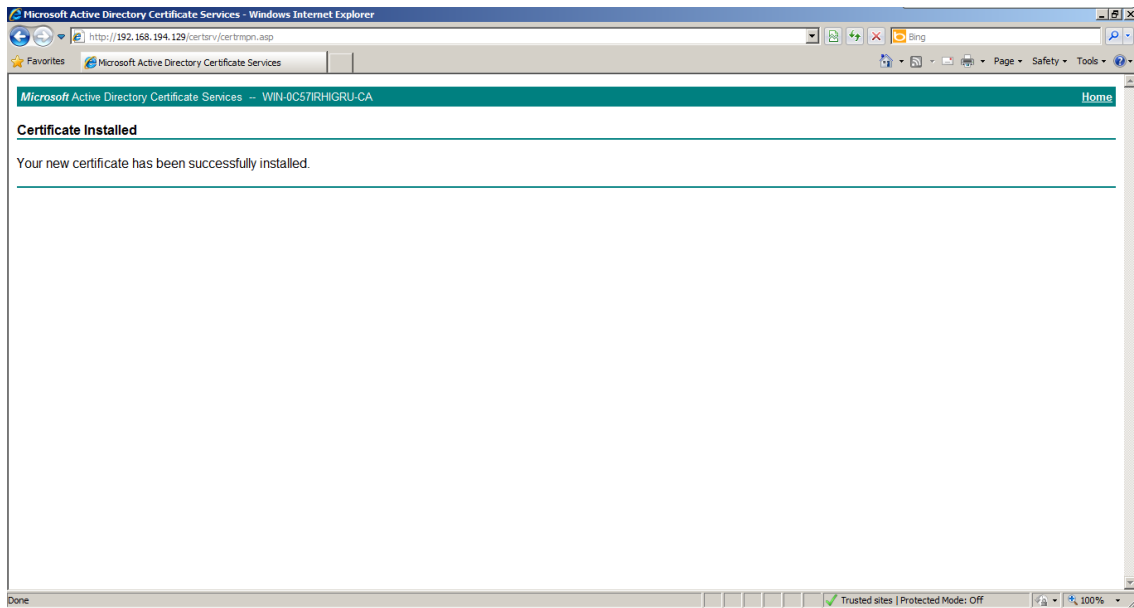


7. Type the correct PIN and click **OK**, a pending certificate page will be displayed, you need to wait for issuer to authenticate and issue you the certificate:



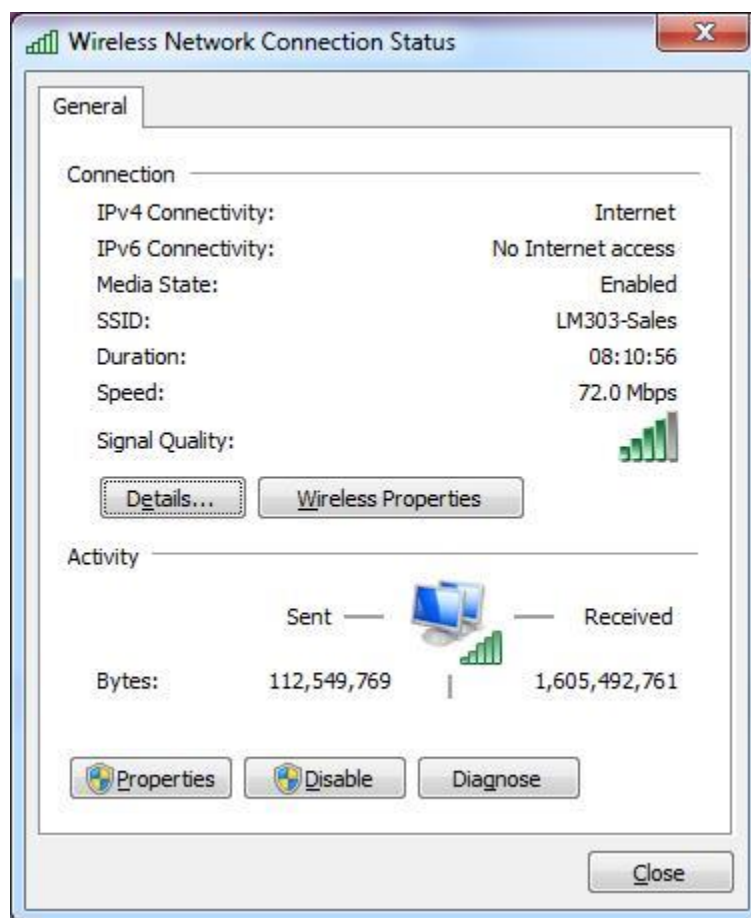
8. Back to **Step 1**, select **view pending certificate request status**. After receiving the notification from your Certificate Authority (CA), you can get the certificate.
9. When installing the certificate, system will also verify your PIN, click **Install this certificate**, you can determine whether the certificate is correctly installed according to the prompts.



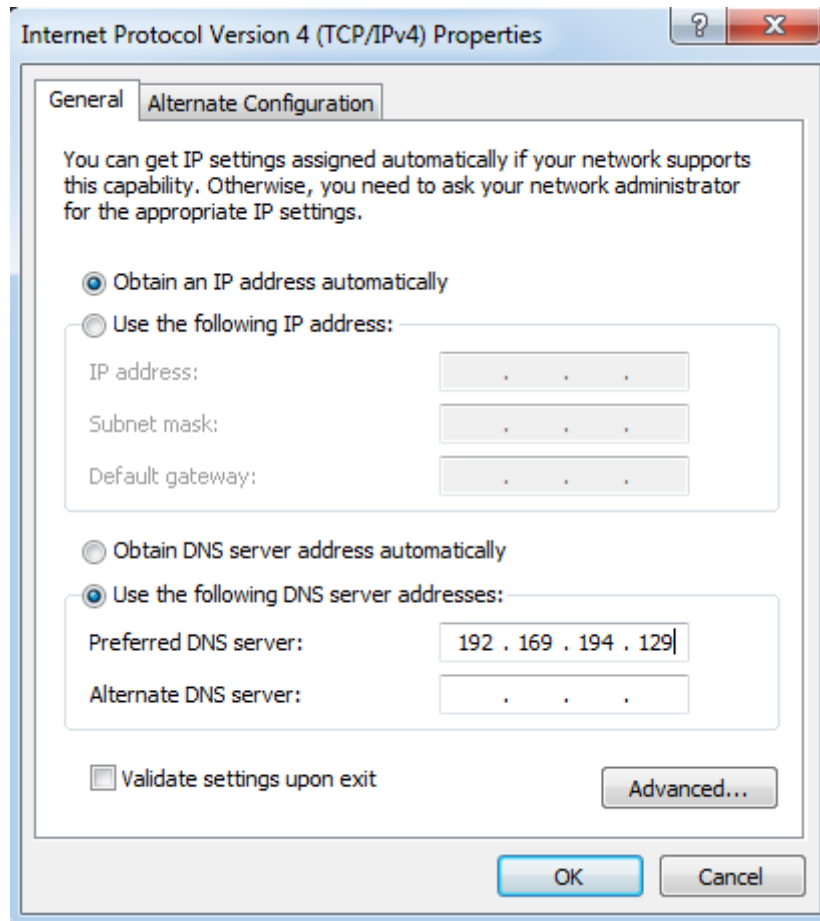


1.2 Smart Card Logon

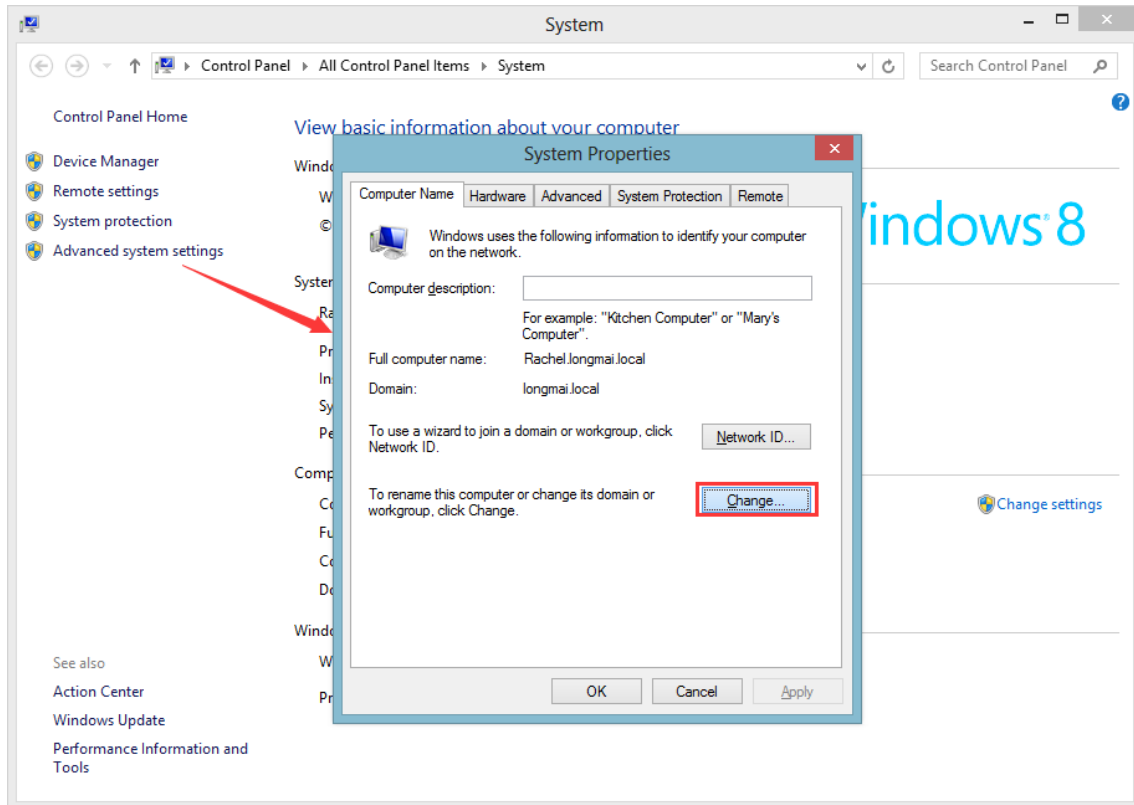
1. Open Wireless Network Connection Status



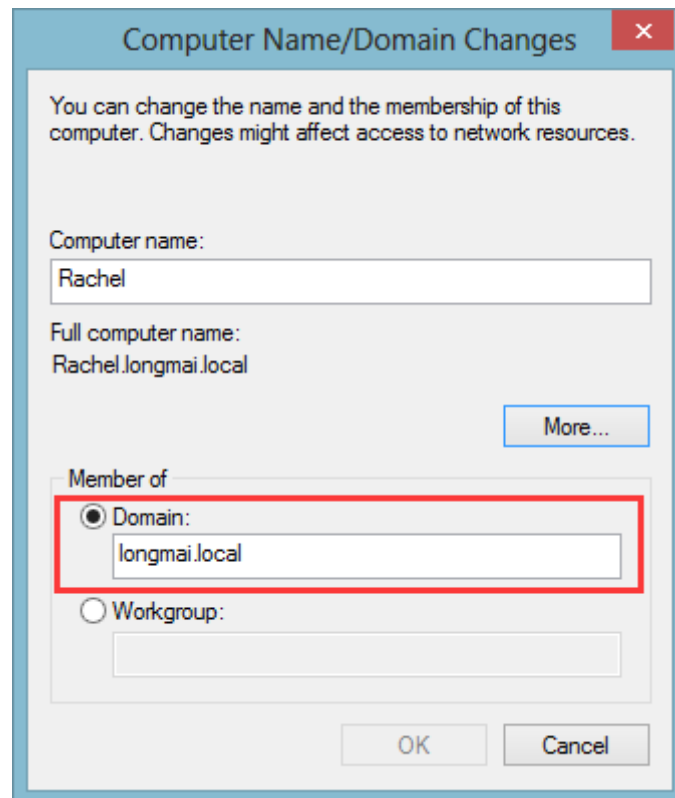
2. Click **Properties** and double-click "*Internet Protocol Version 4(TCP/IPv4)*". Set the Server address, here I will set my server address: as 192.169.194.129



3. Back to the desktop, right-click **Computer**, select **Properties** → **Advanced system settings** → **Change**

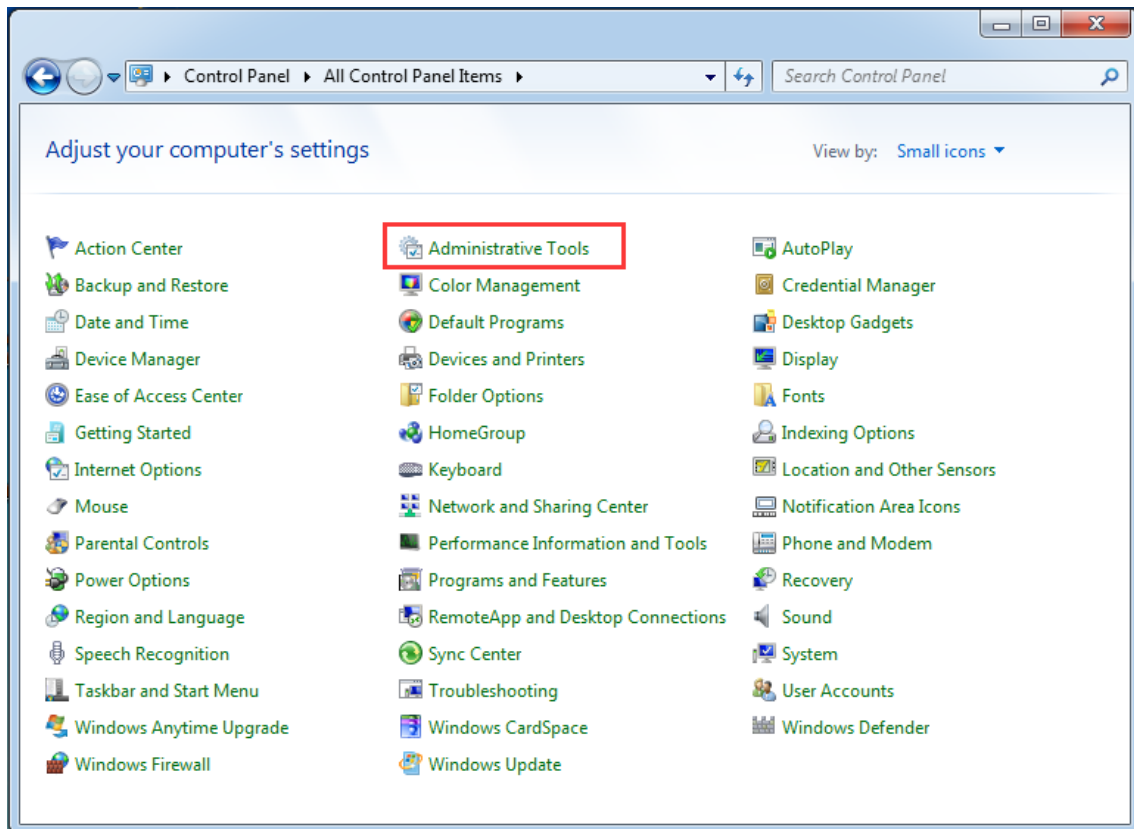


4. Input domain name, here I input longmai.local as my domain name.

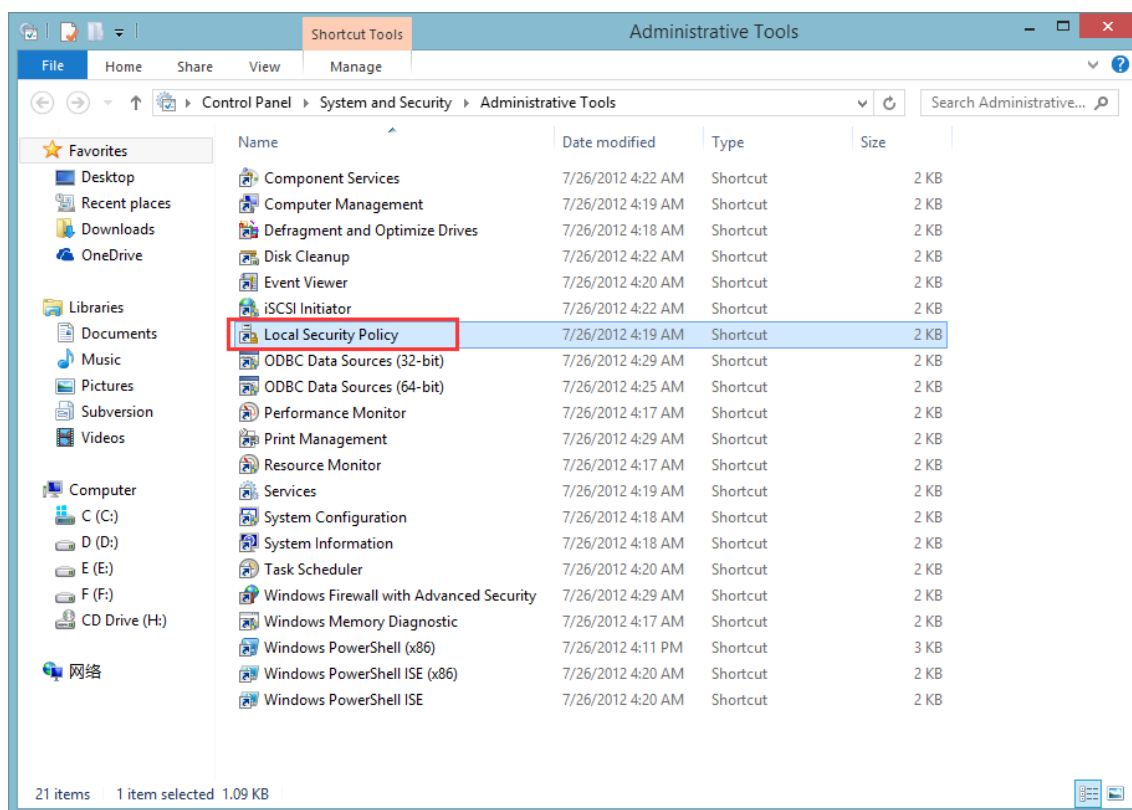


5. Finish all steps, and click **OK** (must input correct domain name and domain password to join in domain successfully).

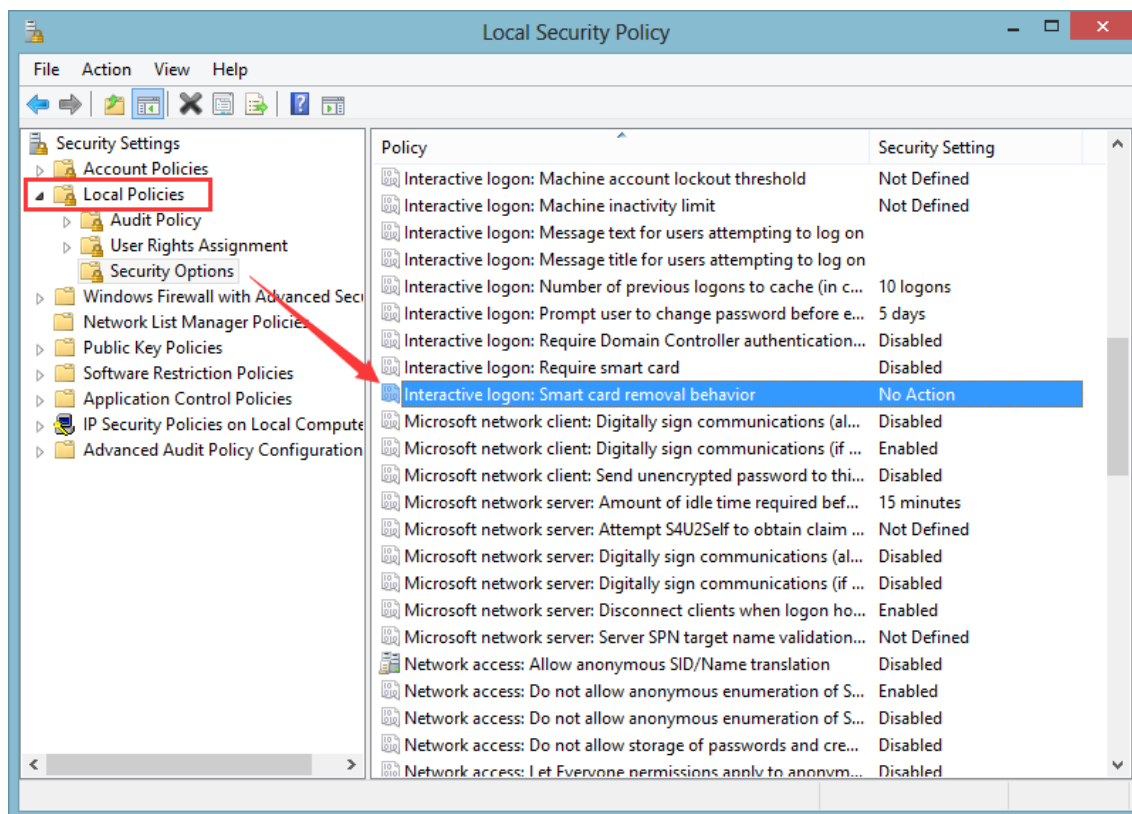
6. Connect your smart card certificate device to the computer.
7. Switch account, login with smart card device.
8. After entering system with smart card device, if you want the system can automatically lock screen after device is unplug from the computer.
Optional: change some local properties - Select **Control Panel** → **Administrative Tools**



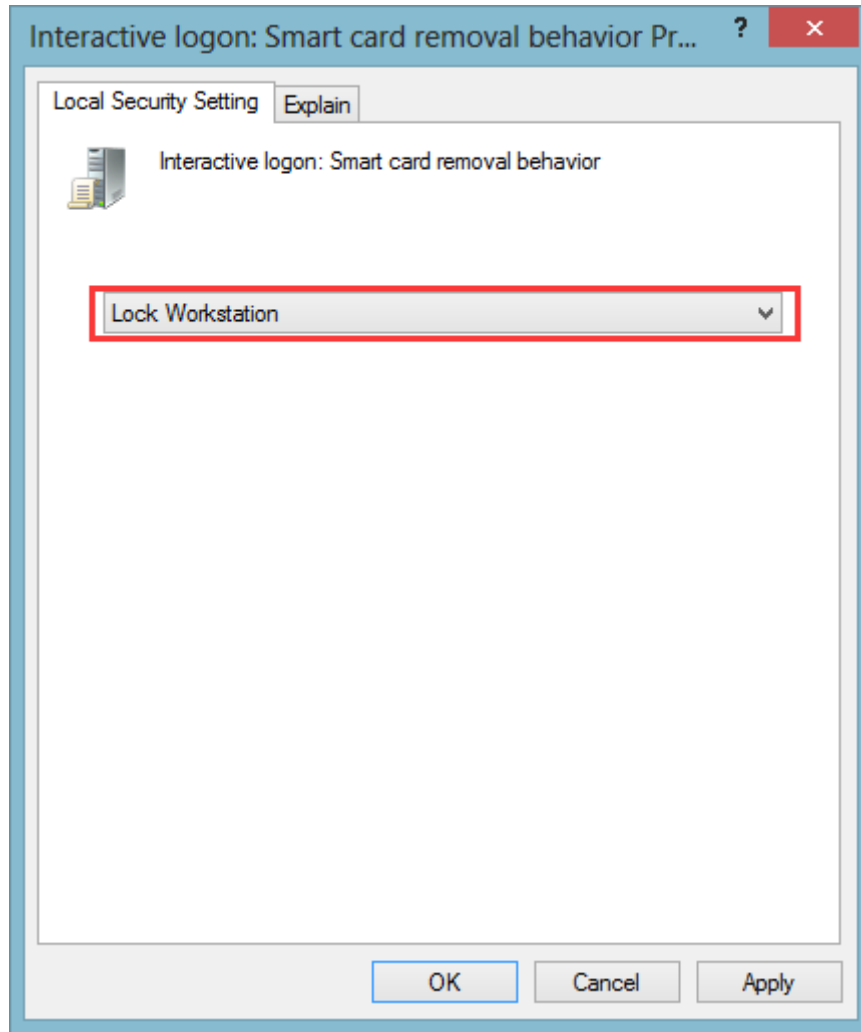
9. Double-Click **Local Security Policy**



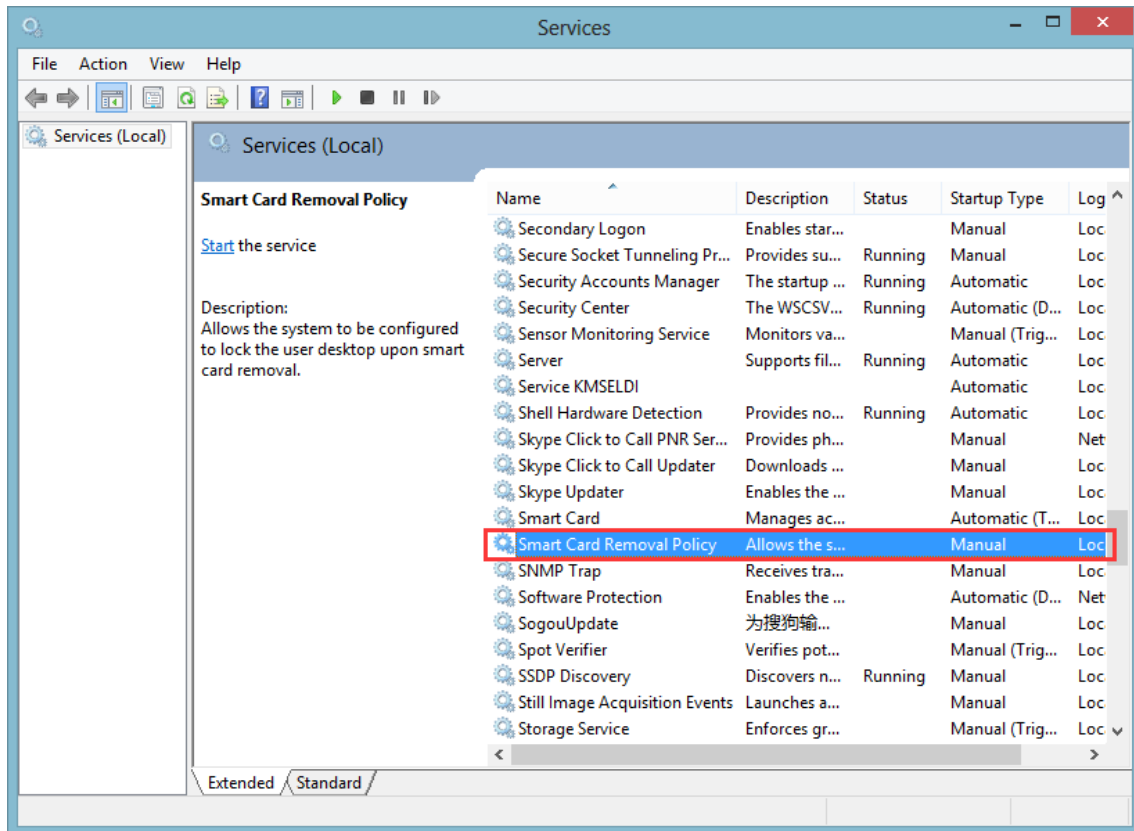
10. Select **Local Policies** → **Security Options** → **Interactive logon: Smart card removal behavior**



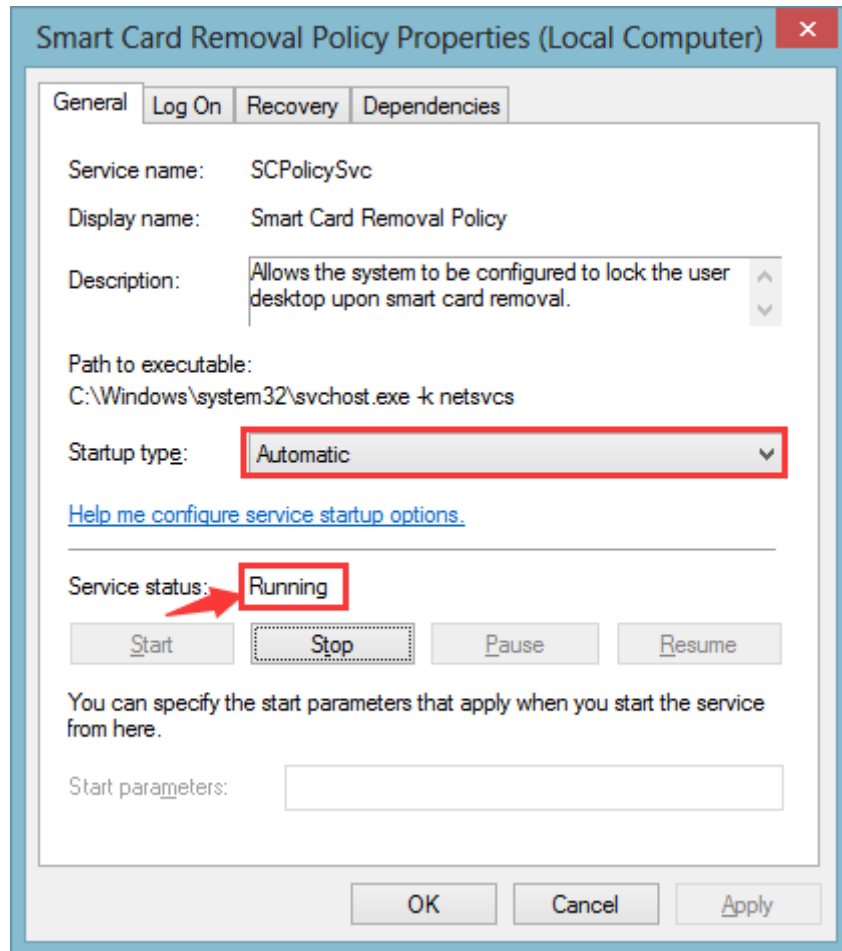
11. Select **Lock Workstation** from drop-down list, click **OK**



12. Then select **Control Panel** → **Administrative Tools** → **Services**, double-click **Smart Card Removal Policy**



13. Select **Automatic** from drop-down list and start service



14. Now the system will lock screen when user unplugs the mToken device.

1.3 Change PIN Code

You can change smartcard PIN code using security desk with Windows Vista and above version systems. Security desk is the most secure working environment in the system. One popular application case is using secure desk to operate Windows user logon. It can also manage other security operations using user proof, such as changing password, Smartcard PIN management, etc.

Follow below steps for changing Smartcard PIN under Windows 7,

1. Press “Ctrl+Alt+Delete” to enter security desk
2. Choose “Changing password”
3. Plug the mToken into the computer.
4. Click “Other Credential ” button
5. Click “smartcard” option
6. Input old PIN, new PIN and then confirm new PIN as follows,



1.4 Unblock Smart Card

This chapter explains how to enable smart card unblocking function, smart card unblocking operations and smart card unblocking admin tool.

Smart card unblock functionality is integrated with Windows Vista and above versions, it is not configured by default, you have to use this function by enabling group policy function. After enable this function, a screen of smartcard unblocking will appeared, and users could unblock smart card by steps.

Enabling unblock smart card

The administrator can use the Group Policy Object Editor snap-in in the Microsoft

Management Console (MMC) to enable unblock from the secure desktop as following steps:

1. Click **Start** button, type **MMC** in the Start Search field and then press **Enter**.
2. When prompted to run Command Prompt as an administrator, click Allow. This will open the Microsoft Management Console dialog.
3. In the Add or Remove Snap-ins dialog box, select Group Policy Object Editor in the Available Snap-ins pane on the left side, and then click Add, as shown in following image:

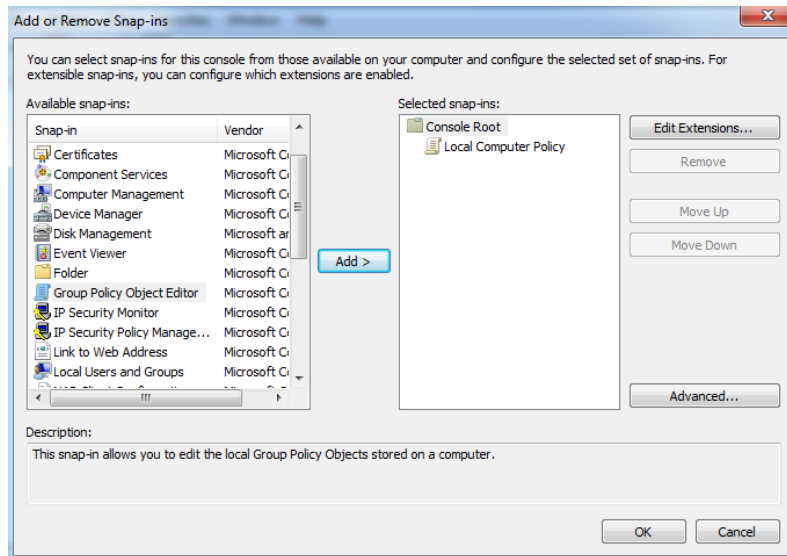


Figure 2, Add Group Policy Object Editor

4. Only local administrator has the right to unblock the computer. Choose “local computer Group Policy Object Editor”, click “Finish” to close the Select Group Policy dialog.
5. Click OK in the Add or Remove Snap-ins dialog box to close it.
6. Click on the Local Computer Policy node in the left side pane, then click on Computer configuration—>Administrative Templates—>Windows Components—>Smart Card. And then double-Click Allow Integrated Unblock screen to be

displayed at time of logon in the Setting list, as shown in following image:

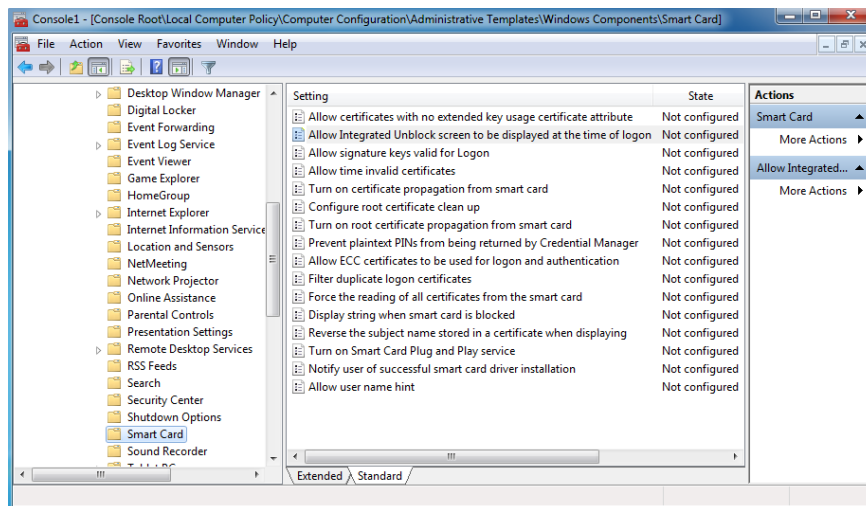
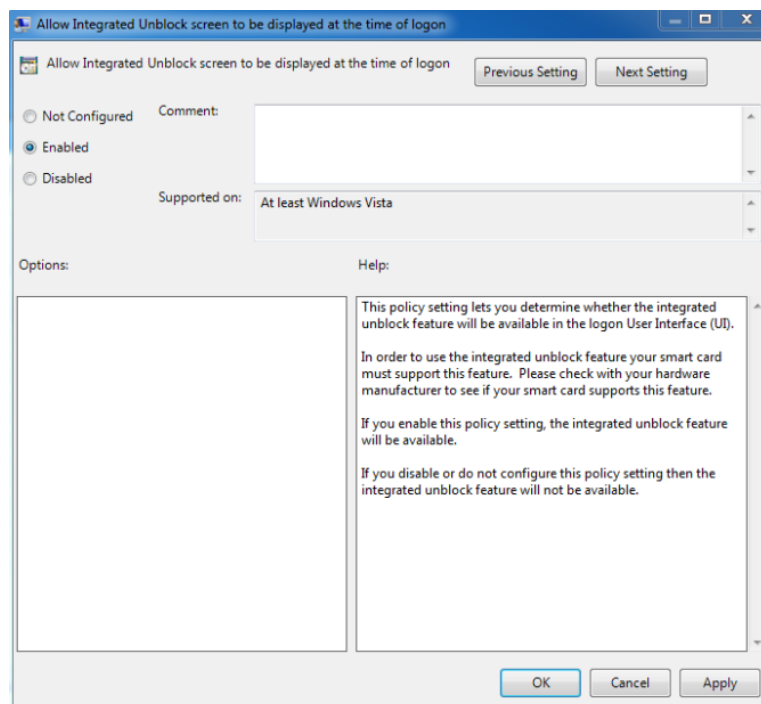


Figure 3, Unblock Smart Card setting

7. Select the Enabled option button, and then click OK, as shown in following image:



8. Return to the Console 1 dialog as step 6, select the Local Computer Policy —> Computer Configuration —> Administrative Templates —> Windows Components —> Smart Card, and double-click on “**Display string when smart card is blocked**” on the right side pane, as shown in following image:

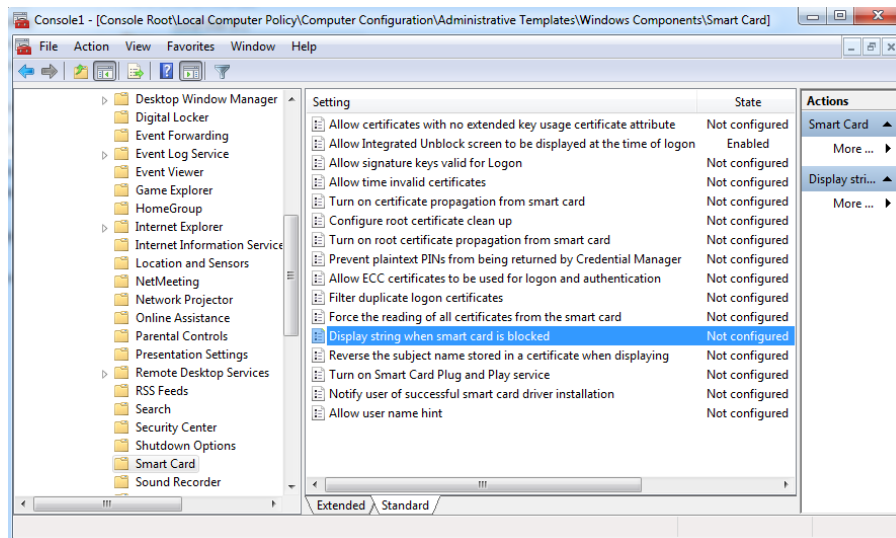


Figure 5, Display string when smart card is blocked Properties

9. Select the Enabled option button and type the string to display on the Unblock screen in the Display sting when smart card is blocked text box, and then press OK, as shown in following image:

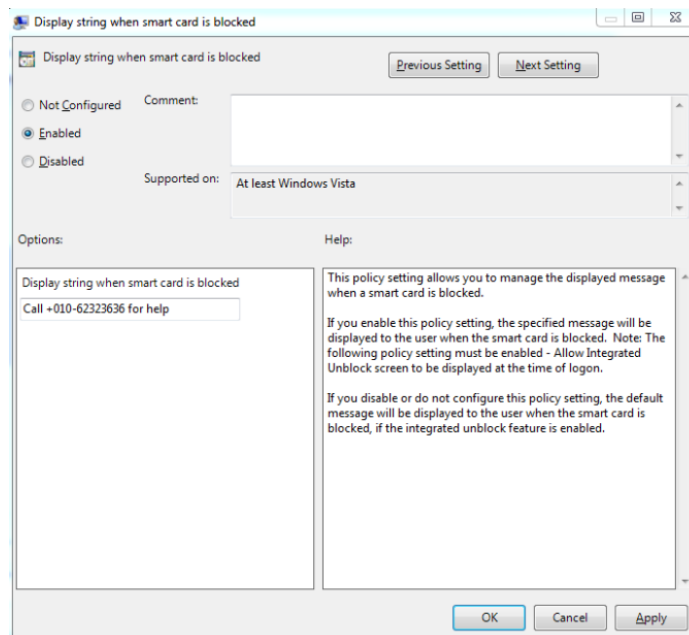


Figure 6, Enable and Input Display string when smart card is blocked Properties

Unblock Smart card

Same as for the Change PIN function, the Smart Card Unblock is integrated into the Windows Vista, 2008 and Windows 7 Secure Desktop. However, it is not configured by default and must be explicitly enabled via Group Policy as 2.2.1 described. When this feature is enabled, the user is presented with the Smart Card Unblock screen when logon is attempted using a blocked smart card, as shown in

following image:



Figure 7, Secure Desktop – Smart Card Unblock

Note: Response code on the above is from Smart card unblock administrator tools.

1.5 Card Unblock Tool

The challenge-response mechanism is used in Windows Smartcard logon for unblocking, the challenge is generated from windows, and response is calculated by the card unblock tool as below:

1. Run the unblock tool, and input SO PIN (default is admin) and challenge code showed on Figure 7 in Challenge textbox (Note: Remove space)
2. Click “Challenge-Response” button to generate response code, as shown in following image:

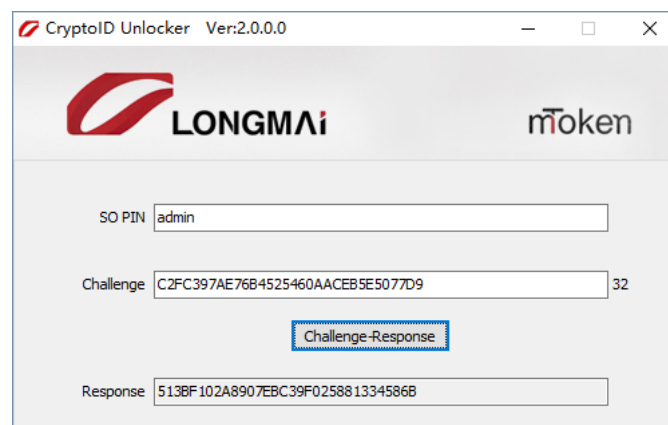


Figure 8, Smart Card Unblock Administrator Tools

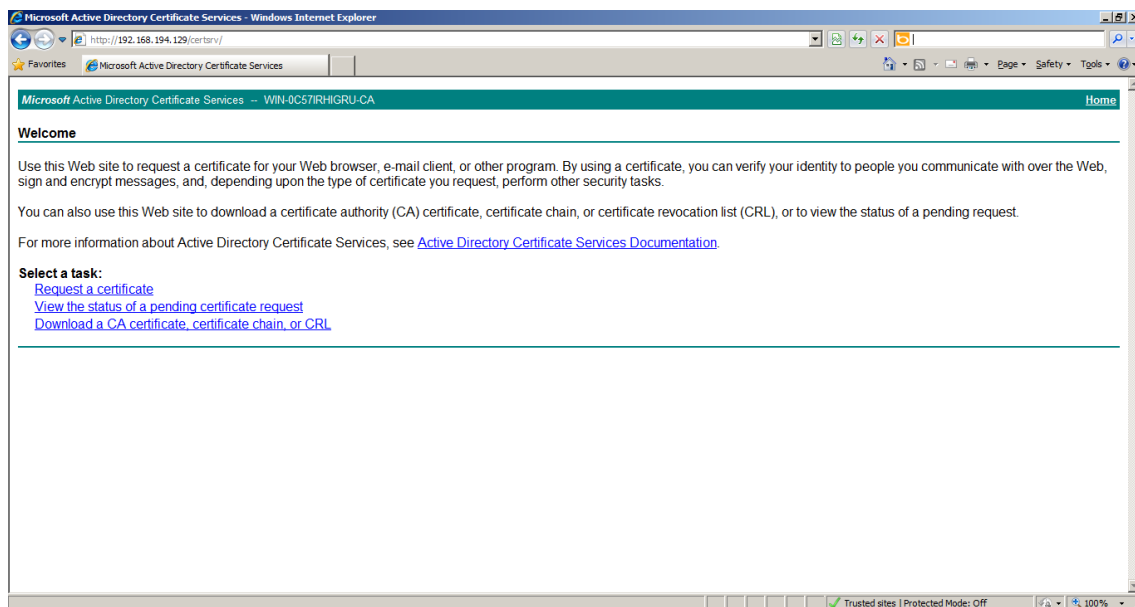
3. Input the generated response code and the new user PIN in the Windows Unblock desktop and click the button to unblock the token.

Chapter 2. BitLocker Drive Encryption

This Chapter mainly describes how to request a BitLocker certificate and how to use mToken CryptoID to encrypt the hard drive.

2.1 Request a BitLocker Certificate

1. Make sure mToken device has been connected to your computer. Then, open the certificate server page through Internet Explorer. (Here I will access my CA Server at <http://192.168.194.129/certsrv/>)



2. Select **Request a certificate** → **Advanced Certificate Request** → **Create and submit an application to the CA**. In Certificate Template Area, select **Bitlocker** template. Select **Microsoft Base Smart Card Crypto Provider** as the CSP.

Certificate Template:

Bitlocker

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: Microsoft Base Smart Card Crypto Provider

Key Usage: ☒ Exchange

Key Size: 1024 Min:1024 Max:2048 (common key sizes: [1024](#) [2048](#))

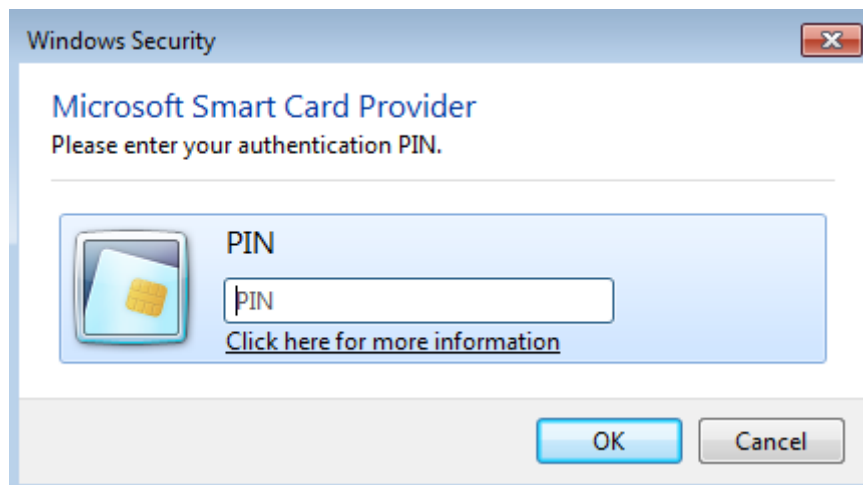
☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

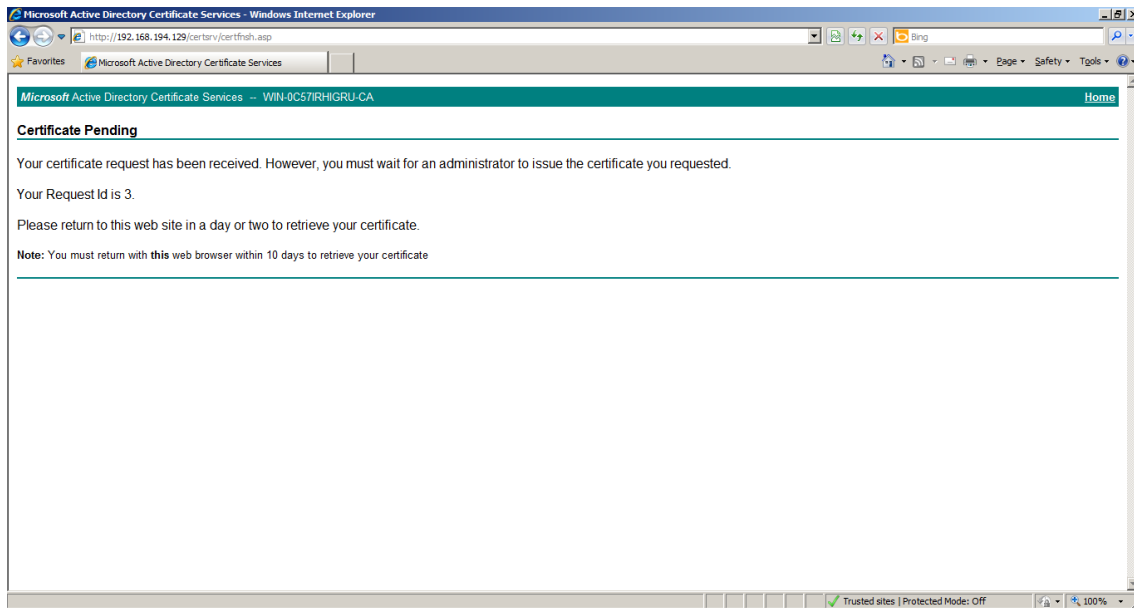
☐ Enable strong private key protection

Additional Options:

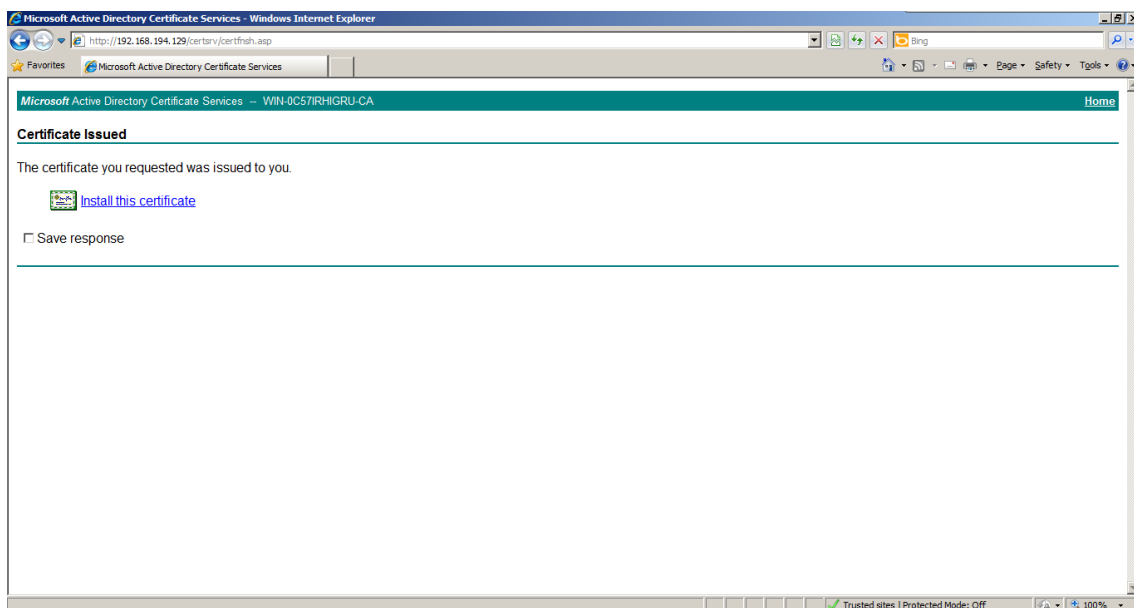
3. Finish the above Settings,click**Submit**, the PIN dialog box pops up.



4. Type the correct PIN and click **OK**, a pending certificate page will be displayed,you need to wait for issuer to authenticate and issue the certificate:

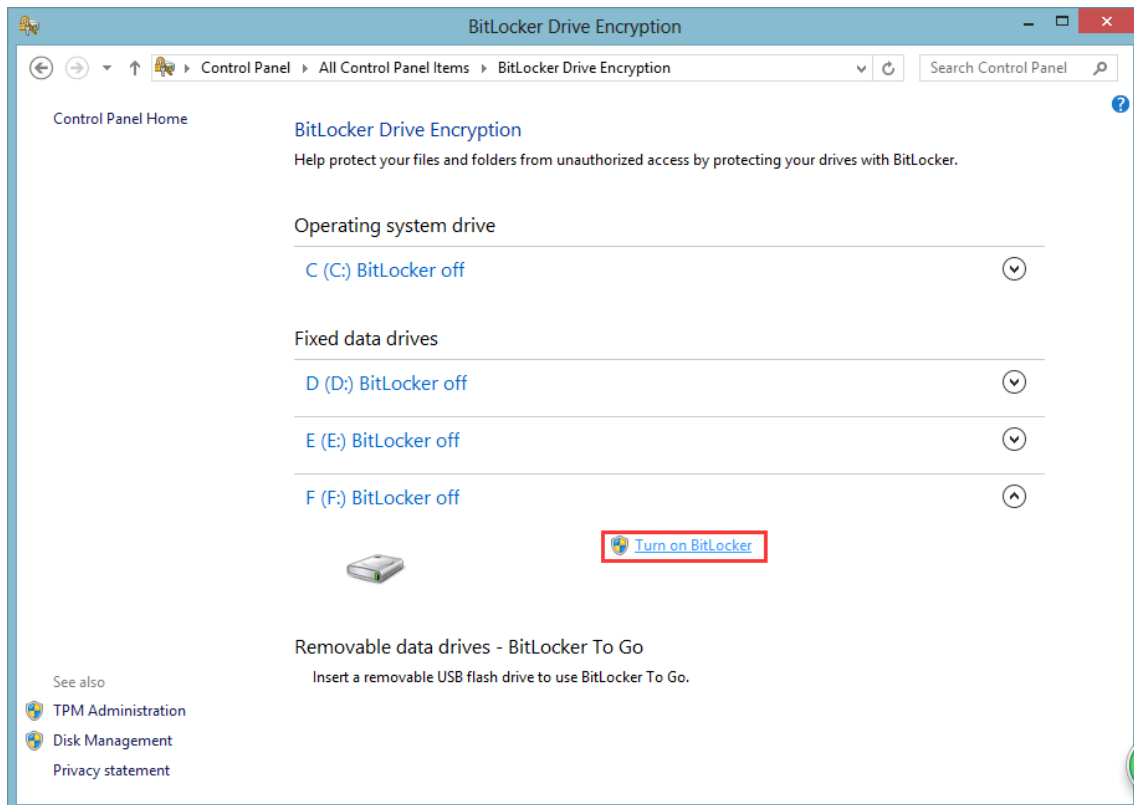
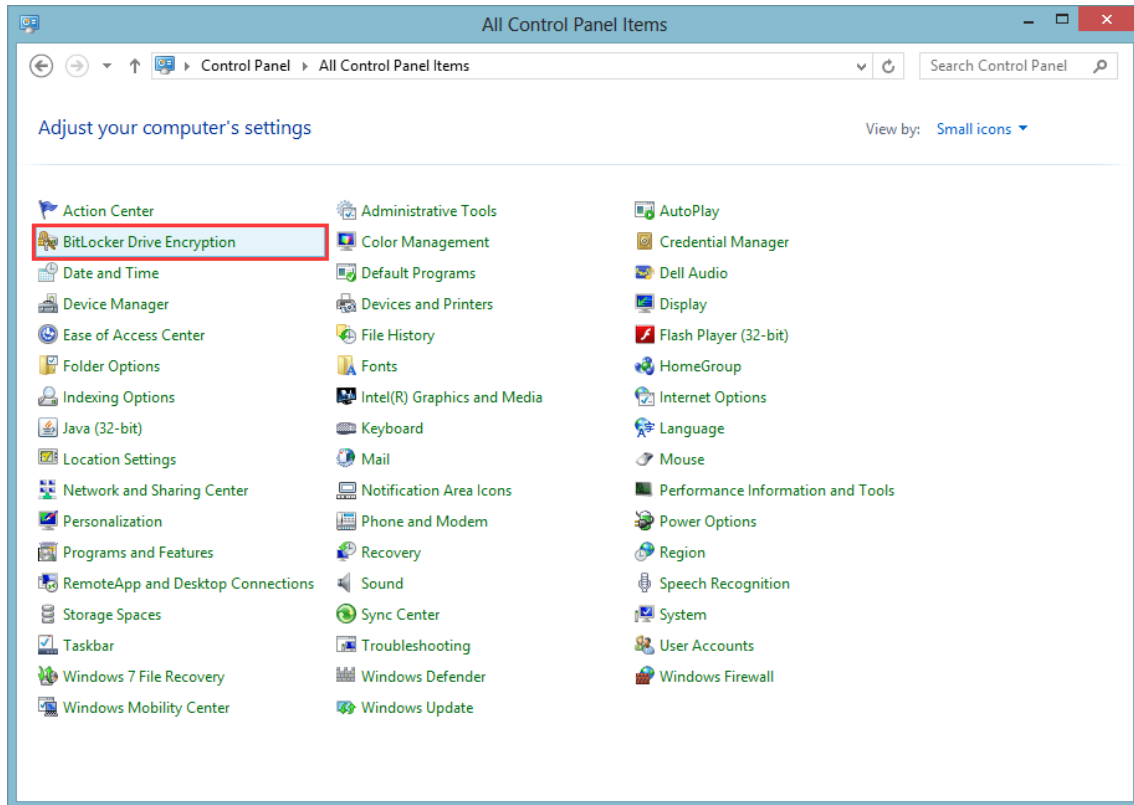


5. Back to **Step 1**, select **view pending certificate request status**. After receiving the notification from the Certificate Authority, you can obtain the certificate. When installing the certificate, system will also verify the PIN, click **Install this certificate**, you can determine whether the certificate is correctly installed according to the prompts.

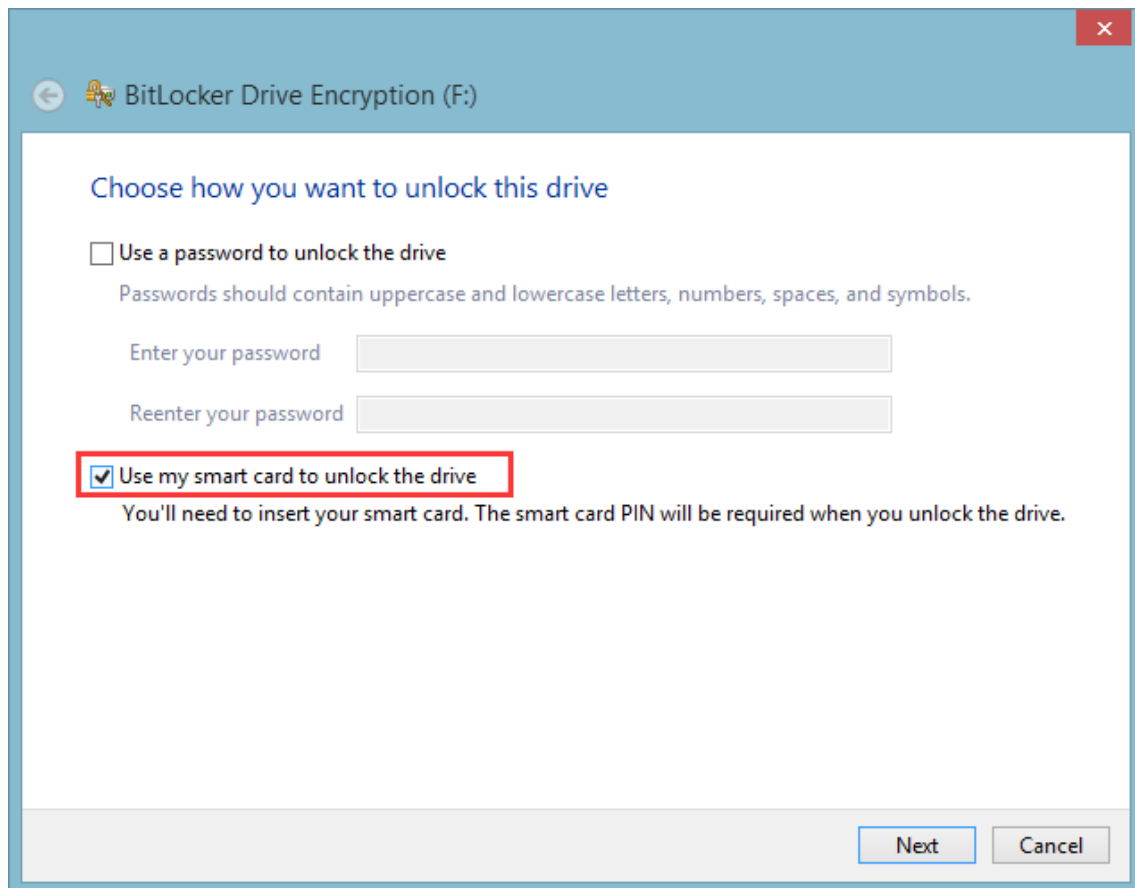


2.2 Drive Encryption

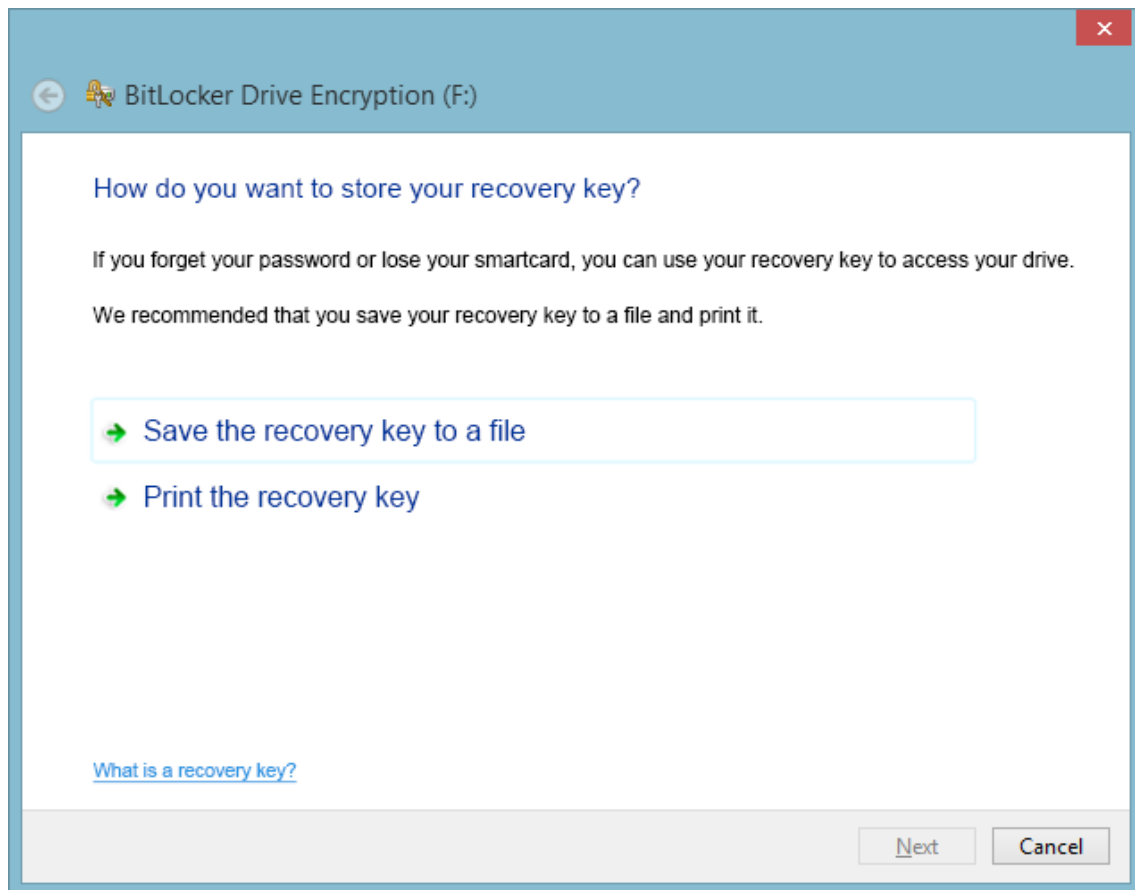
1. Select **Control Panel** → **BitLocker Drive Encryption**, here I will test with encrypting F: disk.
2. **Turn on BitLocker**



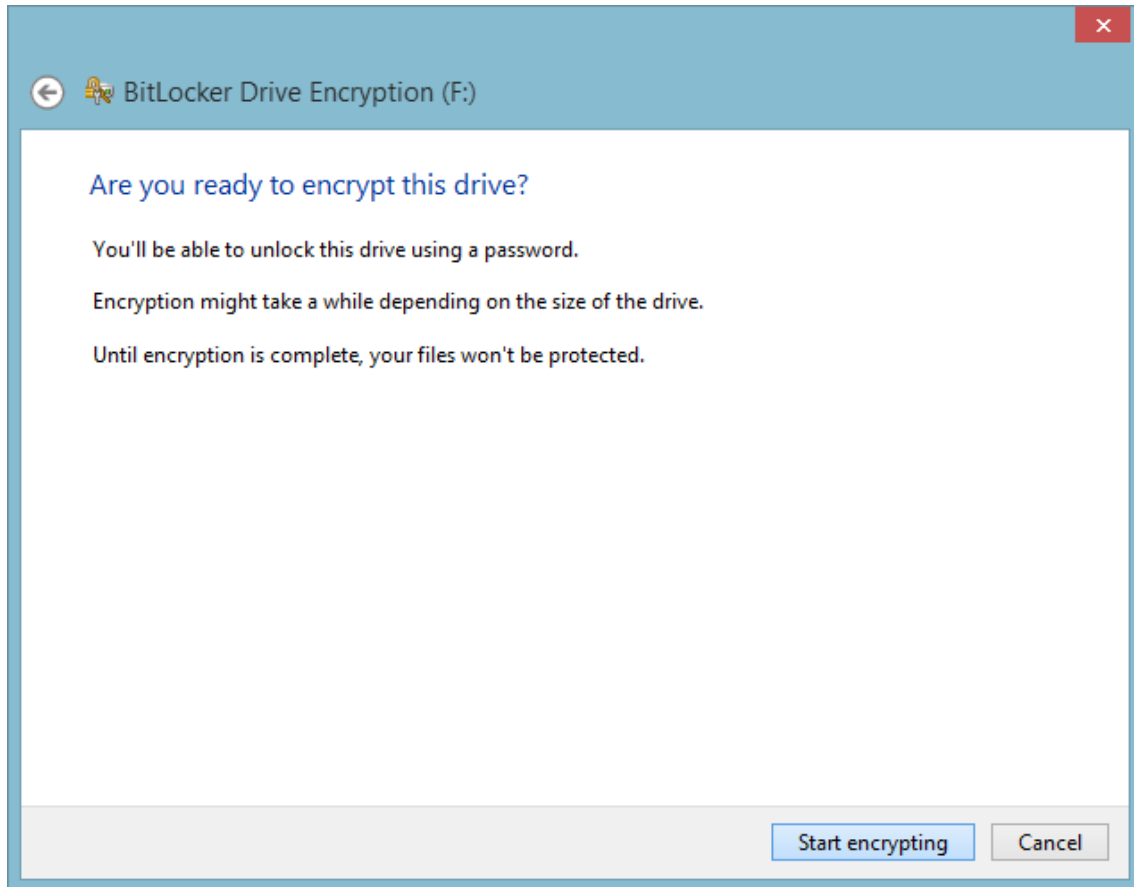
3. Select **Use my smart card to unlock the drive**, click **Next**



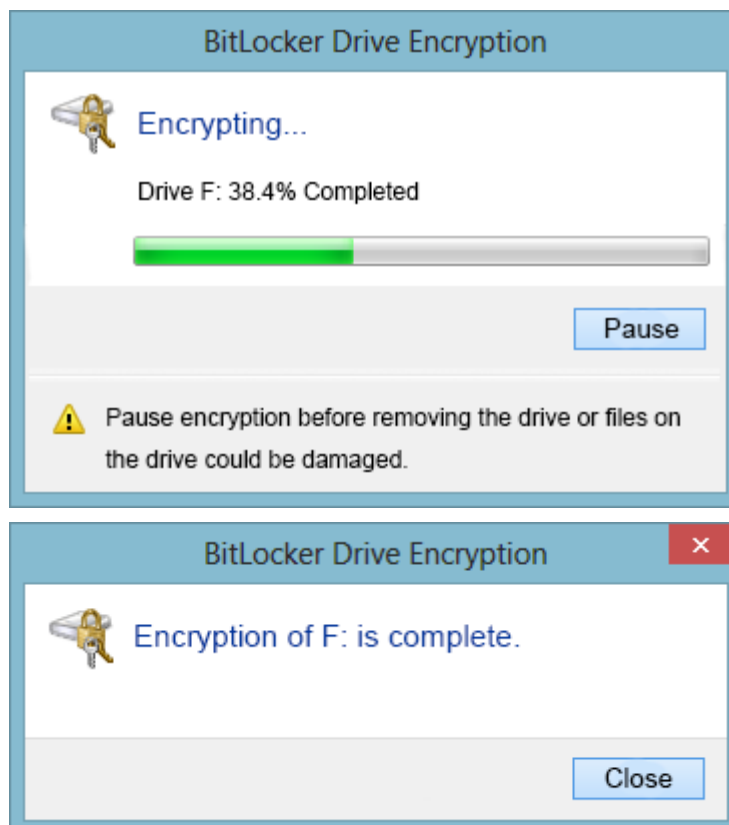
4. Select how to back-up your recovery key



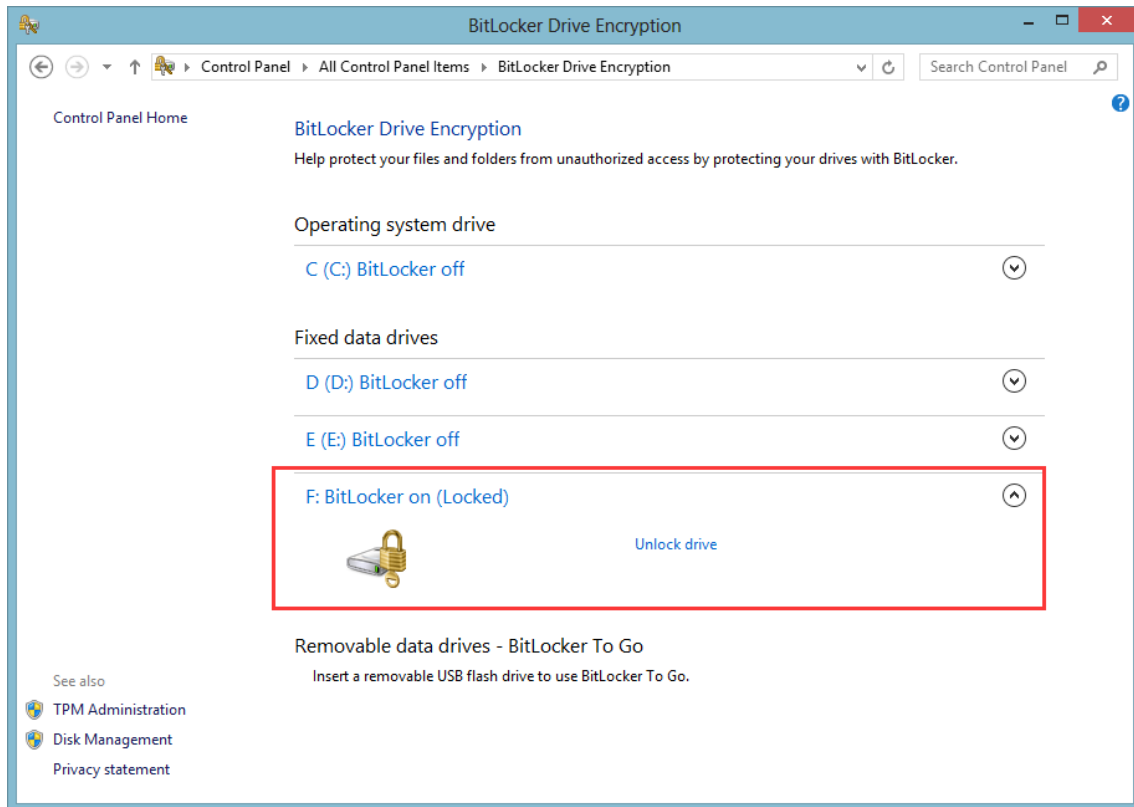
5. Click **Next**, you will see below pop up message.



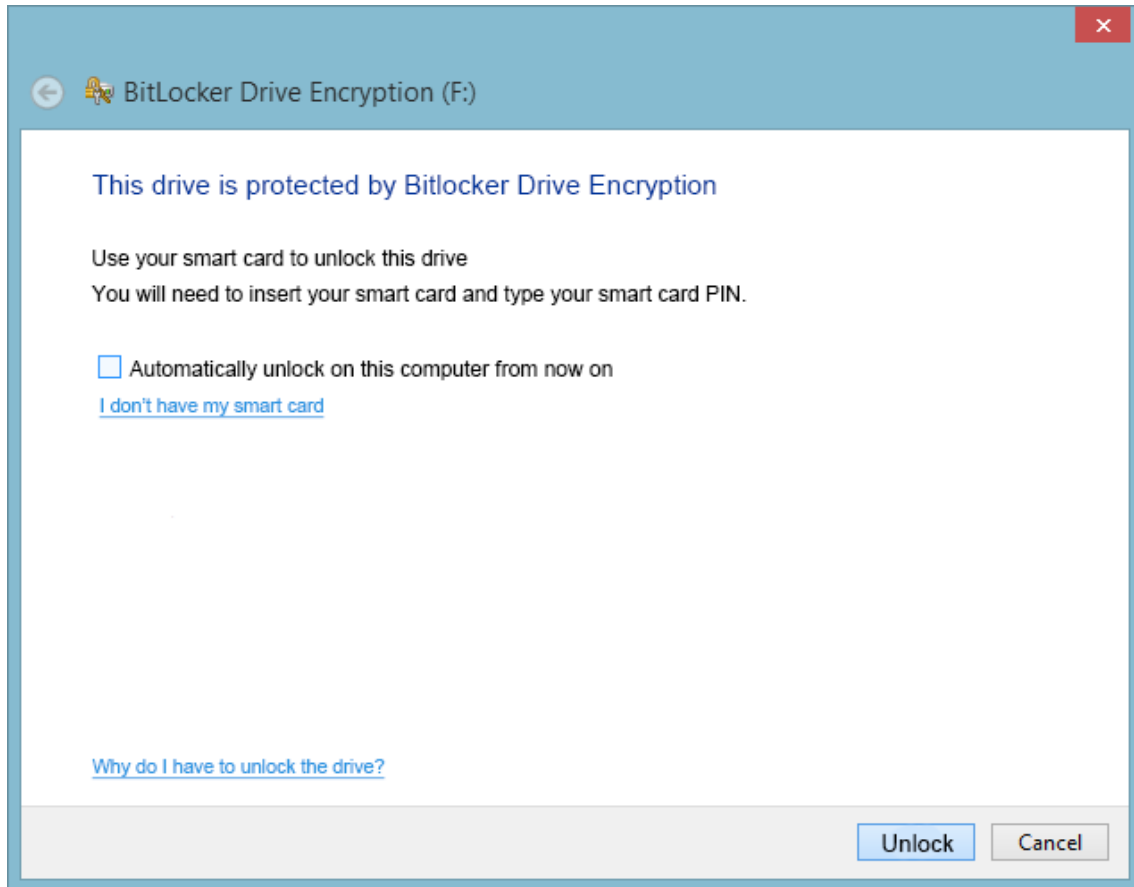
6. Click **Start encrypting**, the encryption progress window will be displayed.



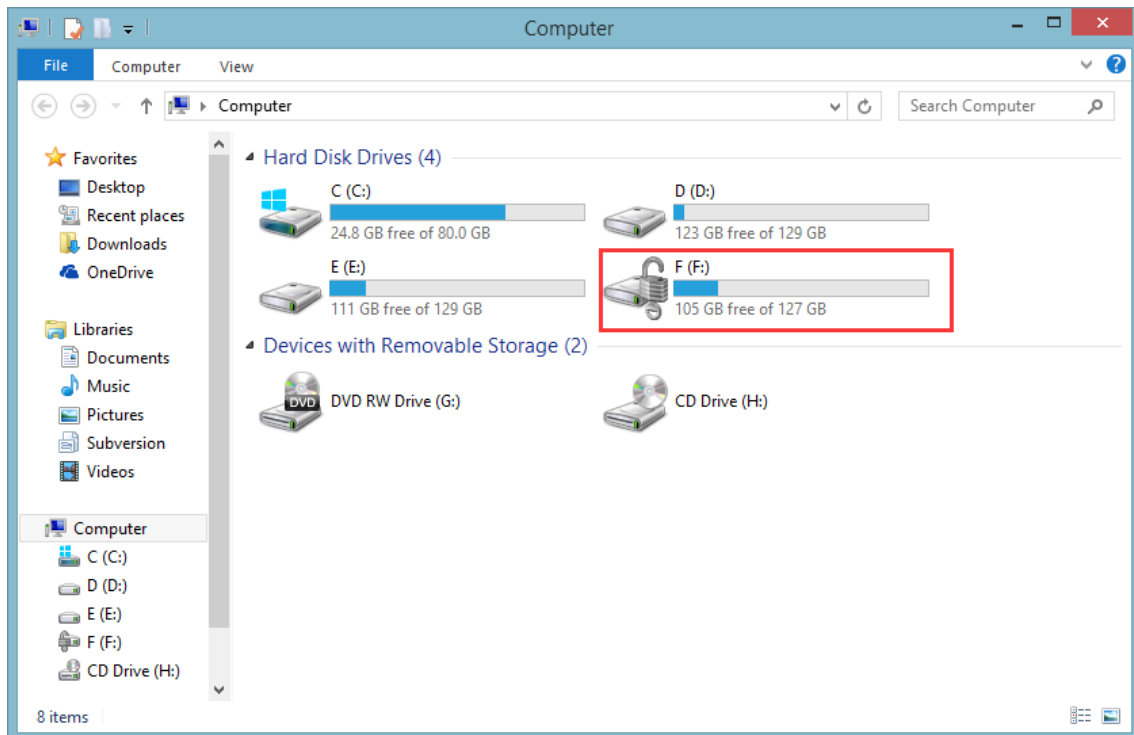
7. You can find the drive has been encrypted



8. To open this drive, you need to first unlock it with smart card



9. Click **Unlock**, input correct device PIN in pop-up window and click OK. The drive is now unlocked and can be accessed normally.



Chapter 3. VPN

mToken CryptoID can be integrated with existing PKI applications seamlessly (the developer needn't to execute any programming tasks except for some corresponding services' configuration).

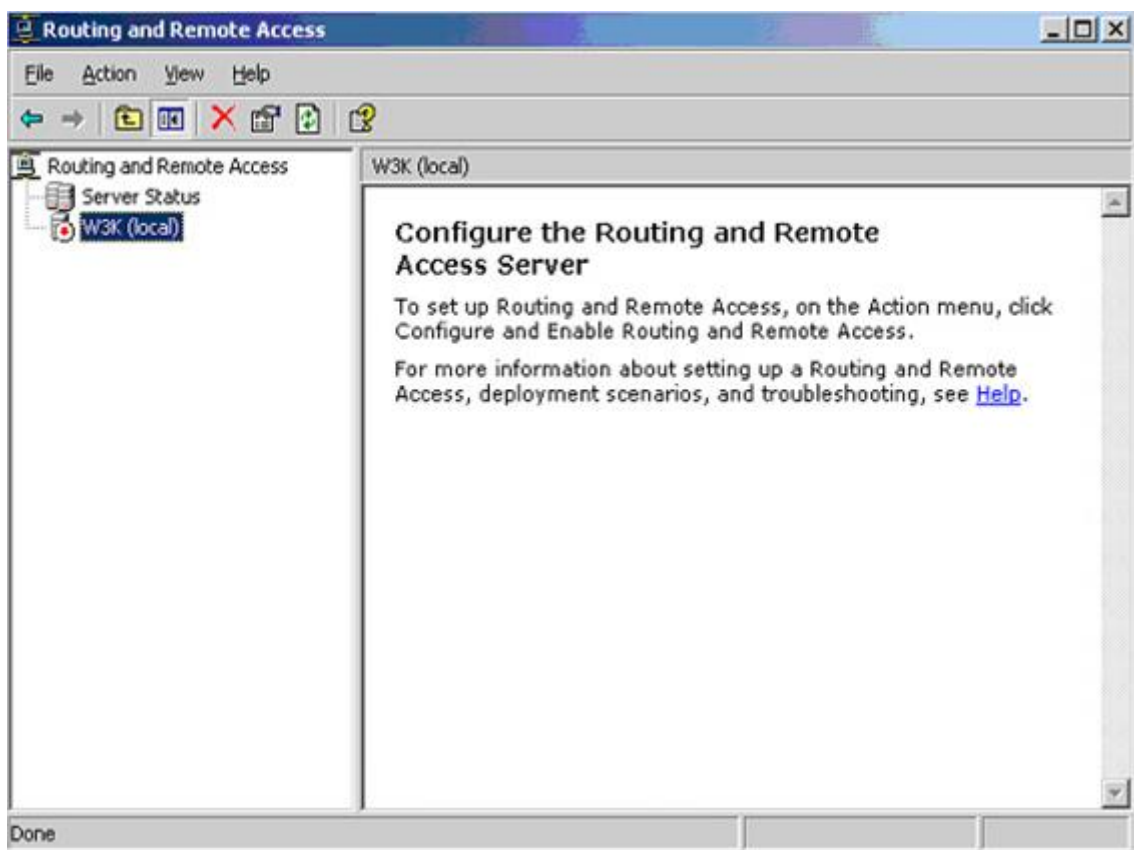
Currently, we can see most PKI applications use PKCS#11 and Crypto API (CAPI) standard interface; CAPI is mainly used on Windows platform while PKCS#11 can be used on cross-platform systems like Windows, Linux as well as Mac OS X.

This chapter mainly describes how to connect VPN with mToken CryptoID.

3.1 Server Configuration

3.1.1 VPN Installation

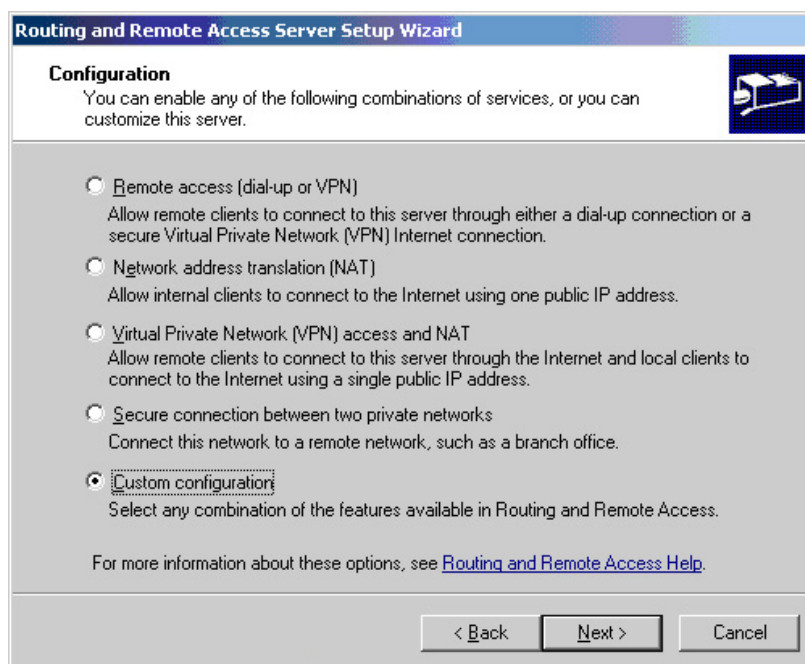
1. Select **Control Panel** → **Administrative Tools** → **Routing and Remote Access**



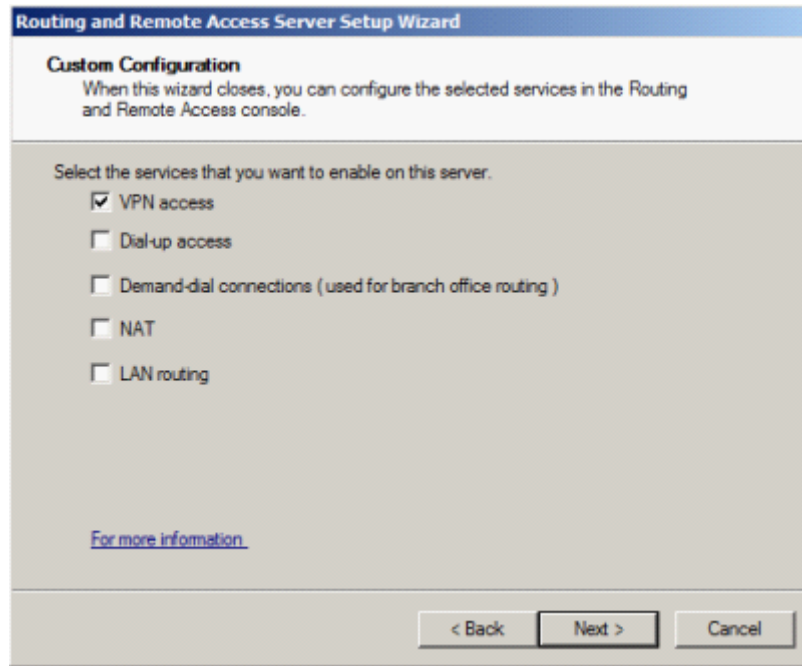
2. Right-Click W3K(local) and select **Configure and Enable Routing and Remote Access**



- Follow the setup wizard and click **Next**, select **Custom configuration**



- Click **Next** and select **VPN access**

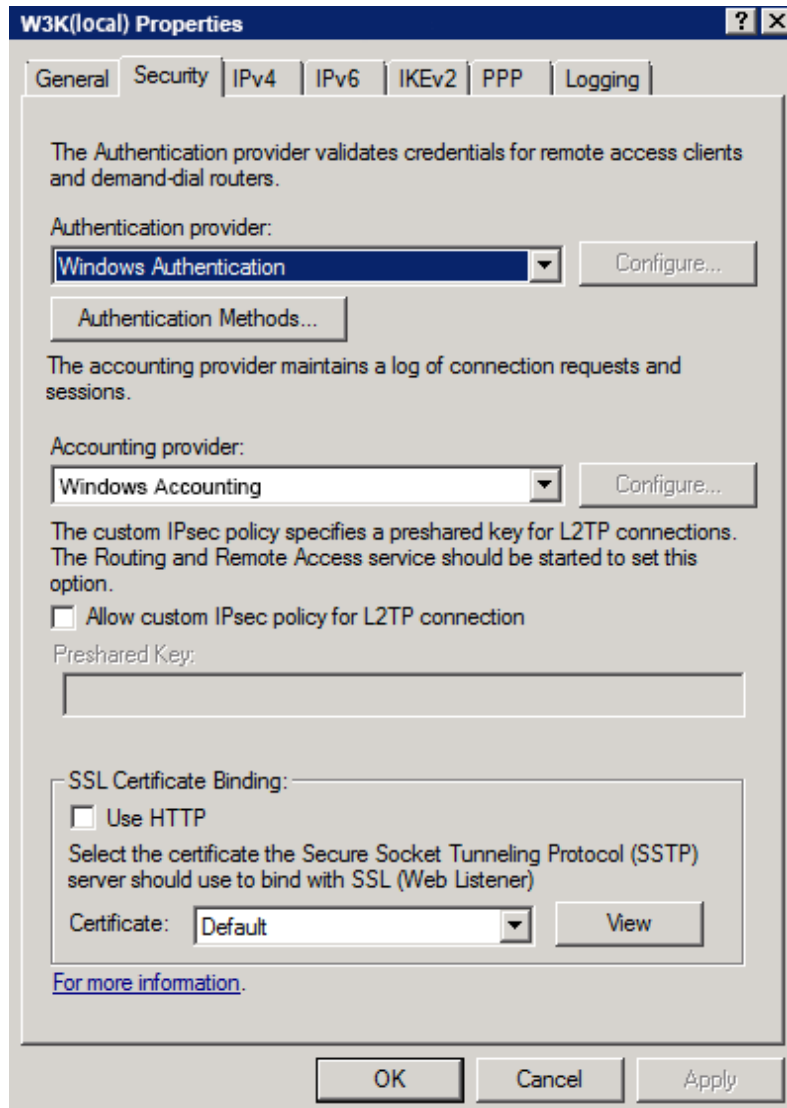


5. Click **Next** and **Finish**

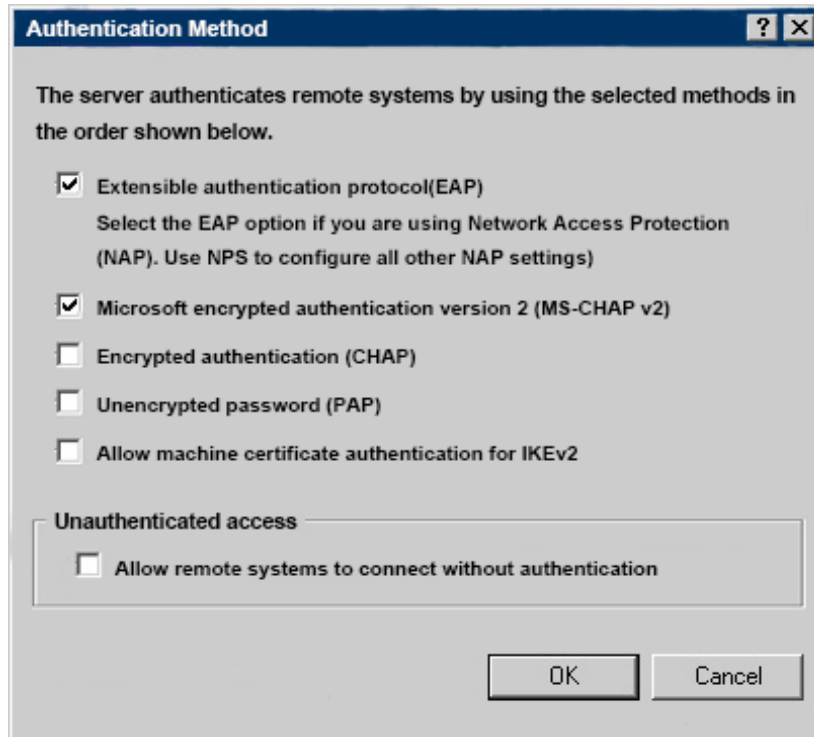


3.1.2 VPN Configuration

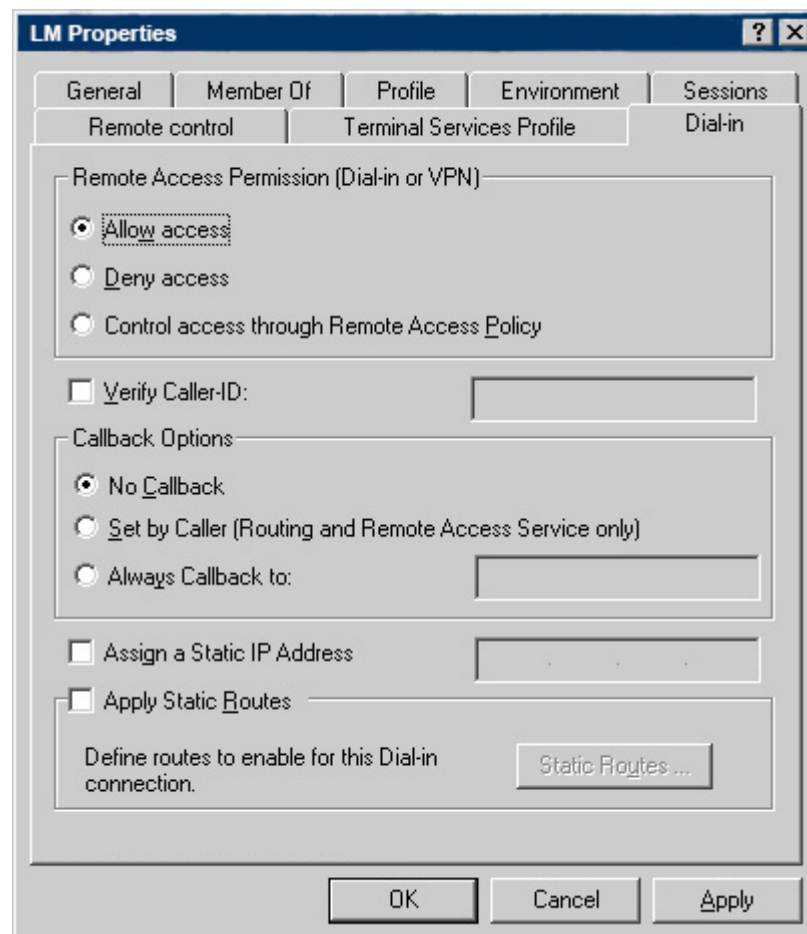
1. Back to **Routing and Remote Access**, right-click W3K(local) and select **Properties** → **Security**



2. Click **Authentication Methods** button, select **Extensible Authentication Protocol** to support smart card identity authentication



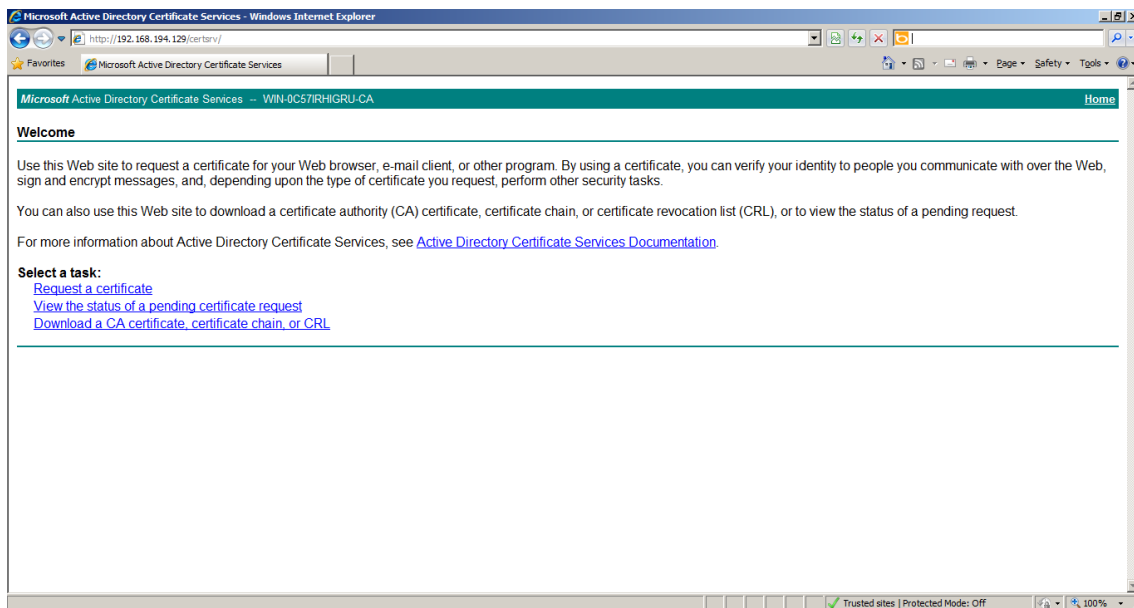
3. Set user permission, allow dial-in VPN



3.2 Client Configuration

3.2.1 Request a Smart Card Logon Certificate

1. Make sure mToken CryptoID device has been connected to your computer. Open the certificate server page through Internet Explorer. (Here I will access my CA Server <http://192.168.194.129/certsrv/>)



2. Select **Request a certificate** → **Advanced Certificate Request** → **Create and submit an application to the CA**. In Certificate Template Area, select smart card related template (Smartcard User or Smartcard Logon). Select **Microsoft Base Smart Card Crypto Provider** as the CSP.

Certificate Template:

Smartcard Logon

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: Microsoft Base Smart Card Crypto Provider

Key Usage: ☒ Exchange

Key Size: 1024 Min:1024 Max:2048 (common key sizes: [1024](#) [2048](#))

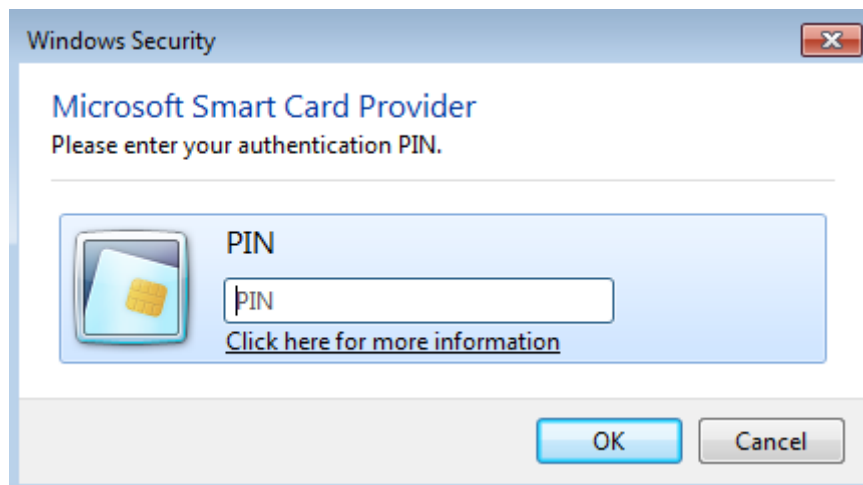
☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

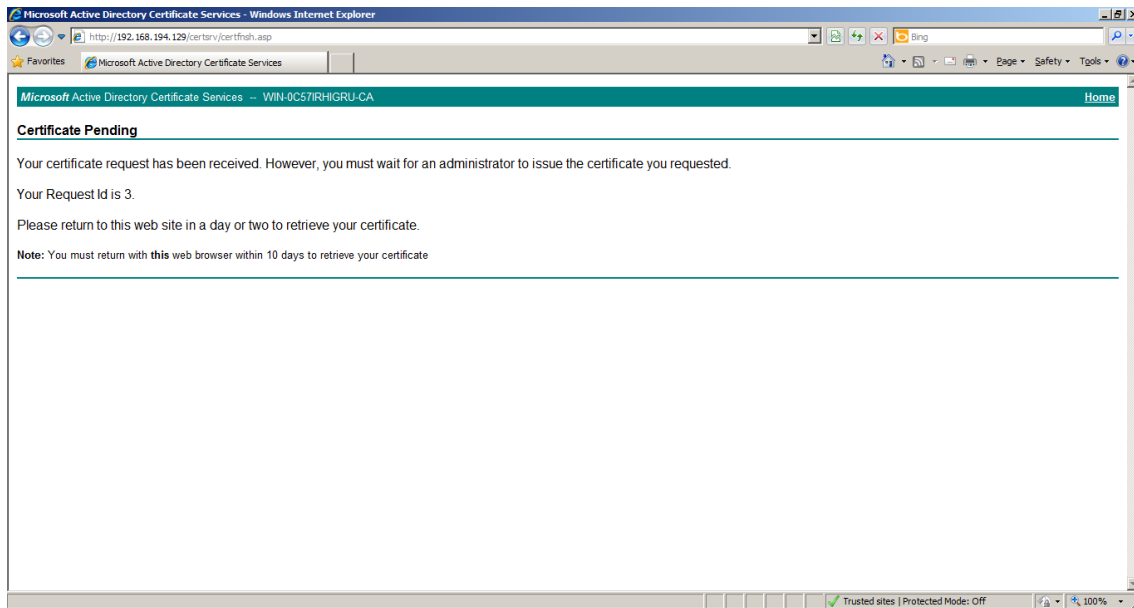
☐ Enable strong private key protection

Additional Options:

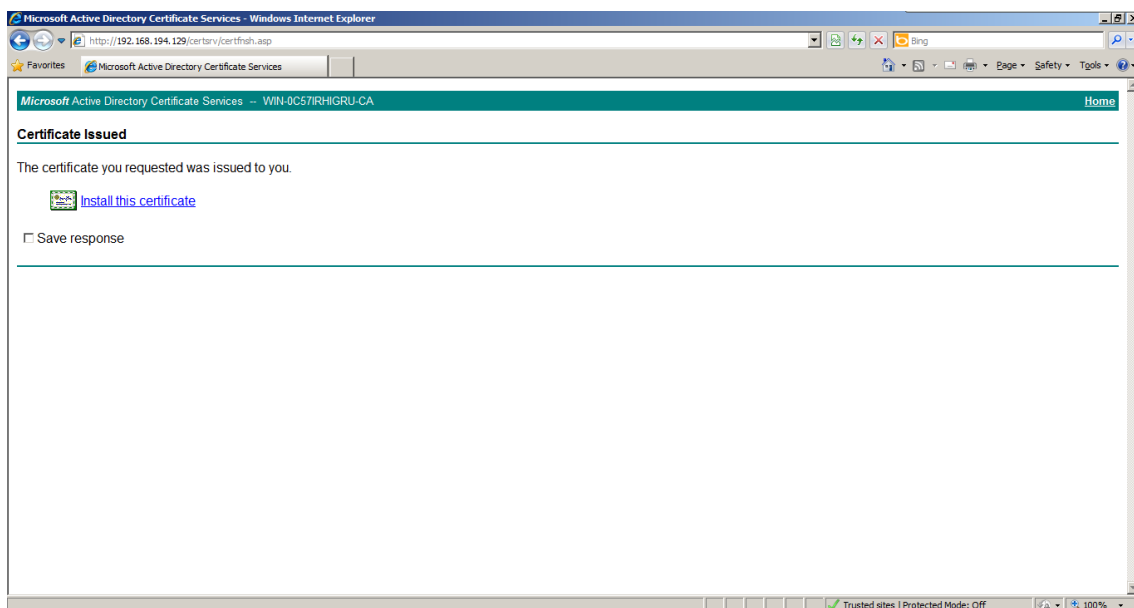
3. Finish the above Settings,click**Submit**, the PIN dialog box pops up.



4. Type the correct PIN and click **OK**, a pending certificate page will be displayed; you need to wait for issuer to authenticate and issue the certificate:

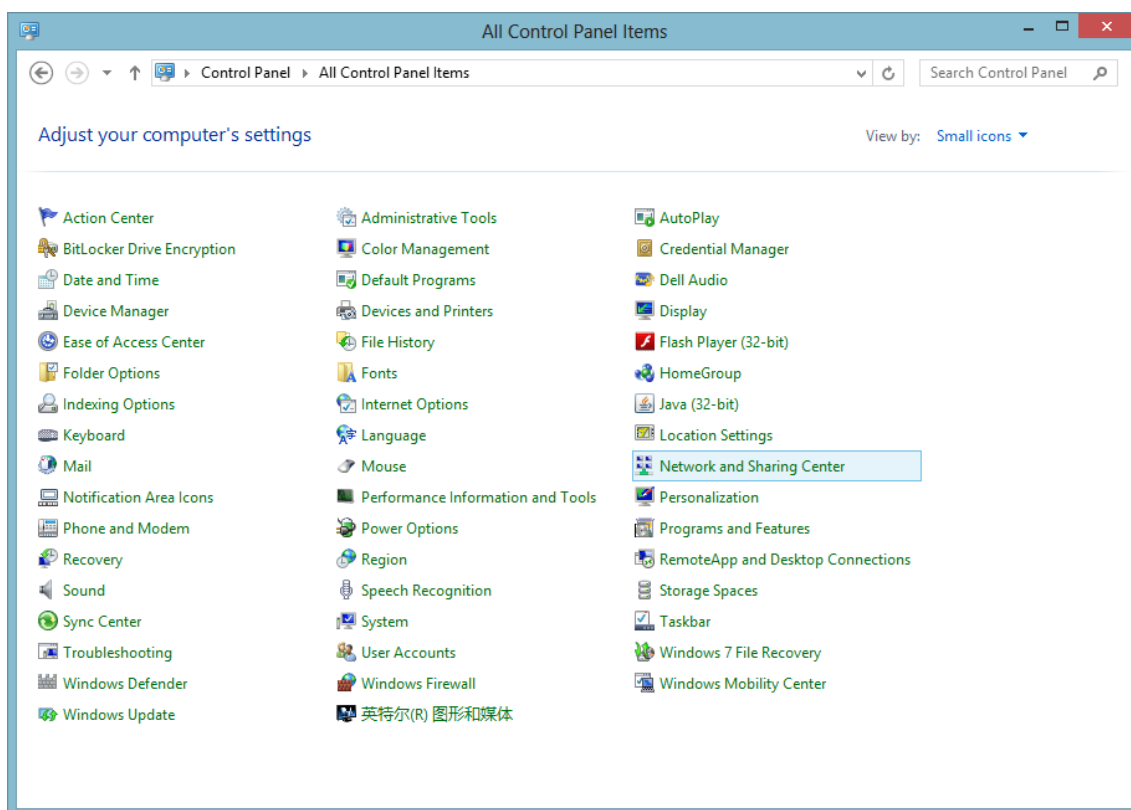


5. Back to **Step 1**, select **view pending certificate request status**. After receive the notification from the Certificate Authority, you can get the certificate. When installing the certificate, system will also verify the PIN, click **Install this certificate**, you can determine whether the certificate is correct installed according to the prompts.

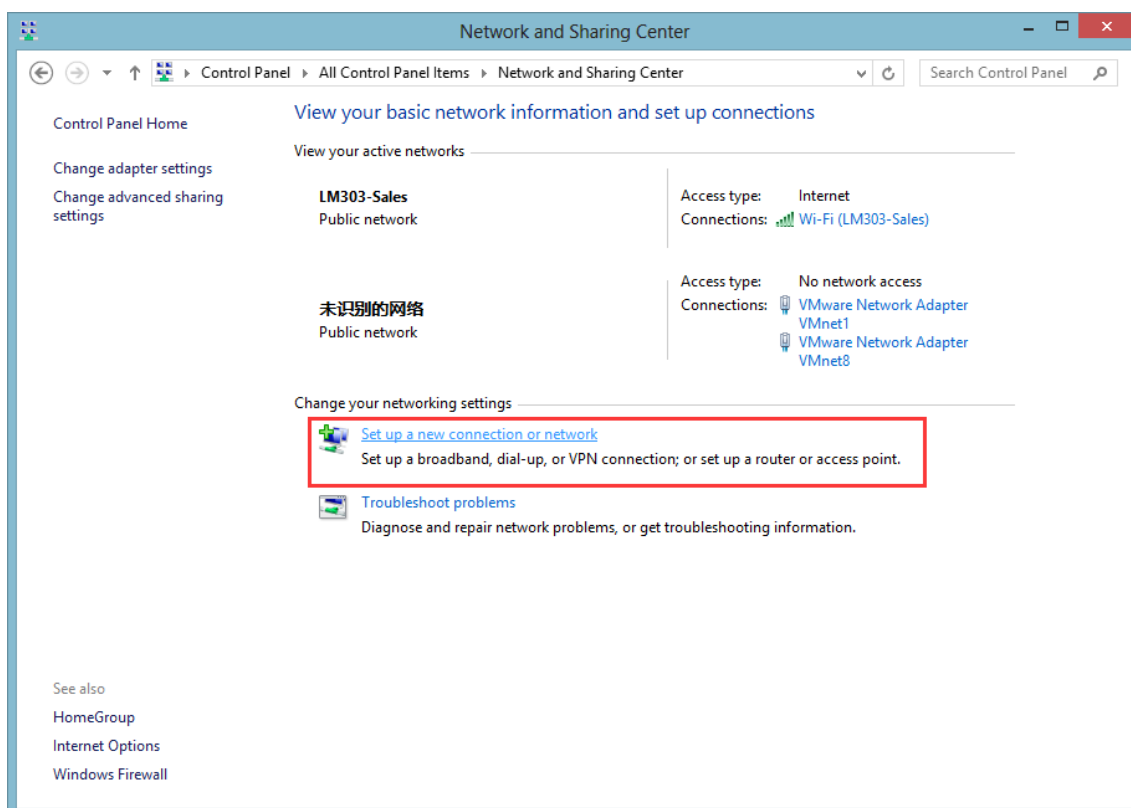


3.2.2 Establish Connection

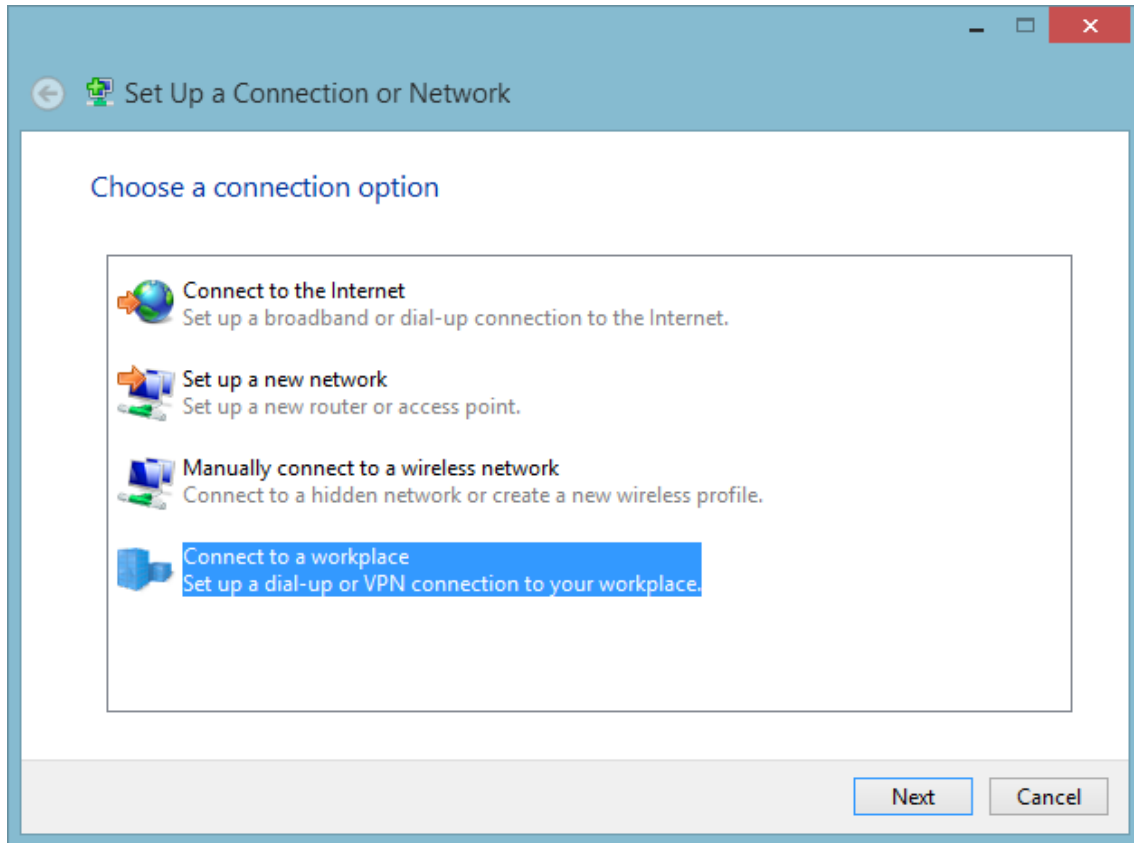
1. Select **Control Panel** → **Network and Sharing Center**



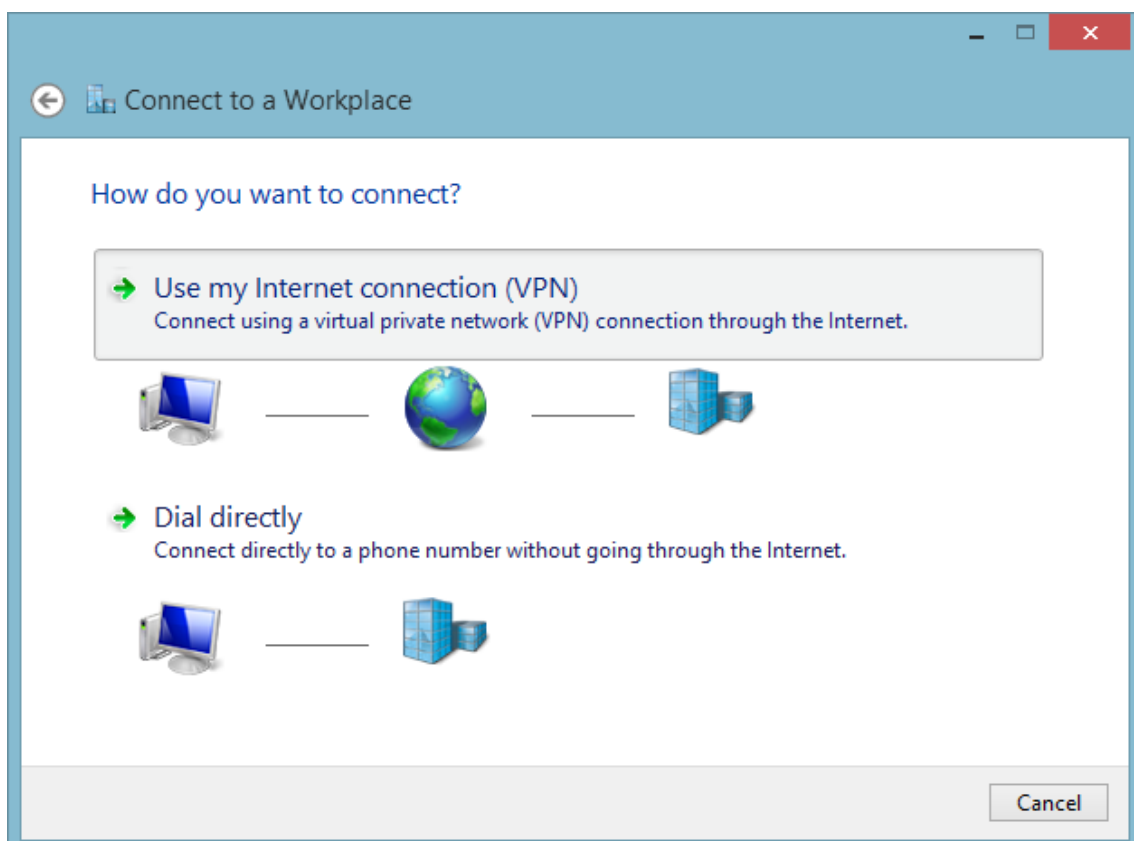
2. Select **Set a new connection or network**



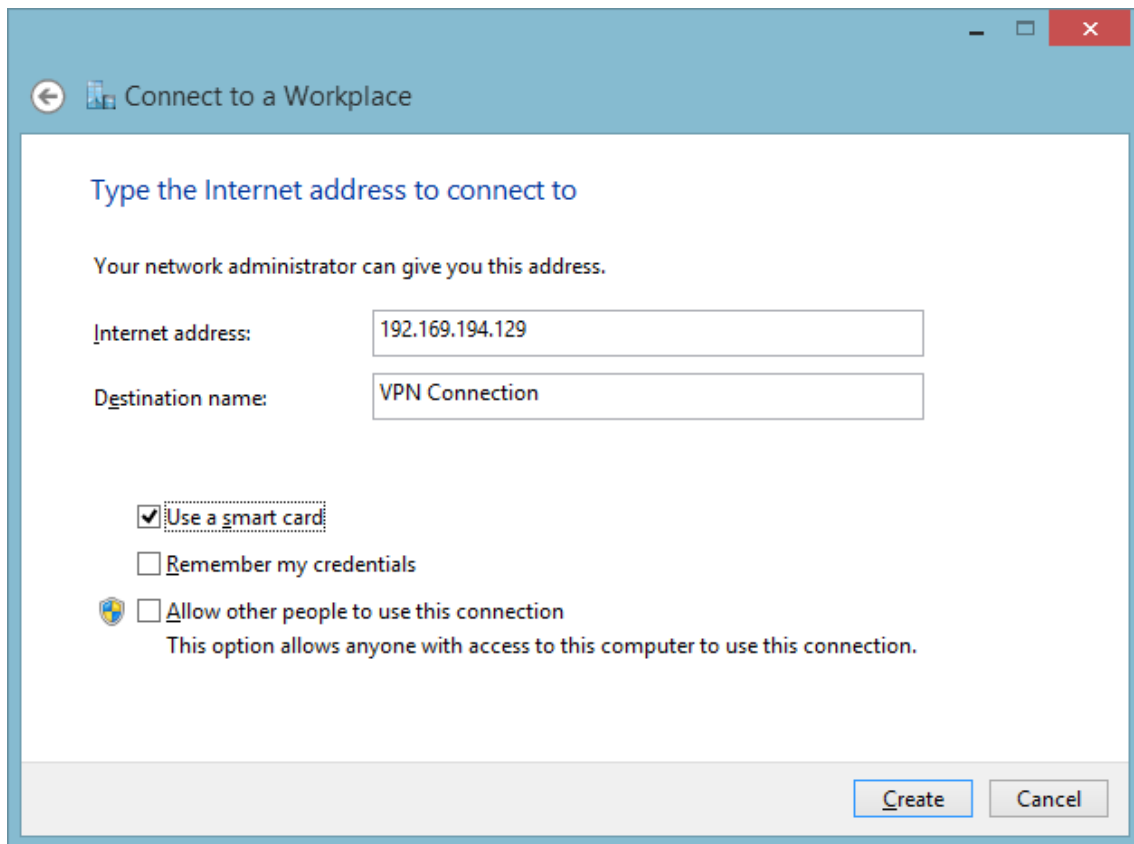
3. Select **Connect to a workplace**, click **Next**



4. Select **Use my Internet connection(VPN)**



5. Type the server address and select Use a smart card, click **Create**



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 192.169.194.129

Destination name: VPN Connection

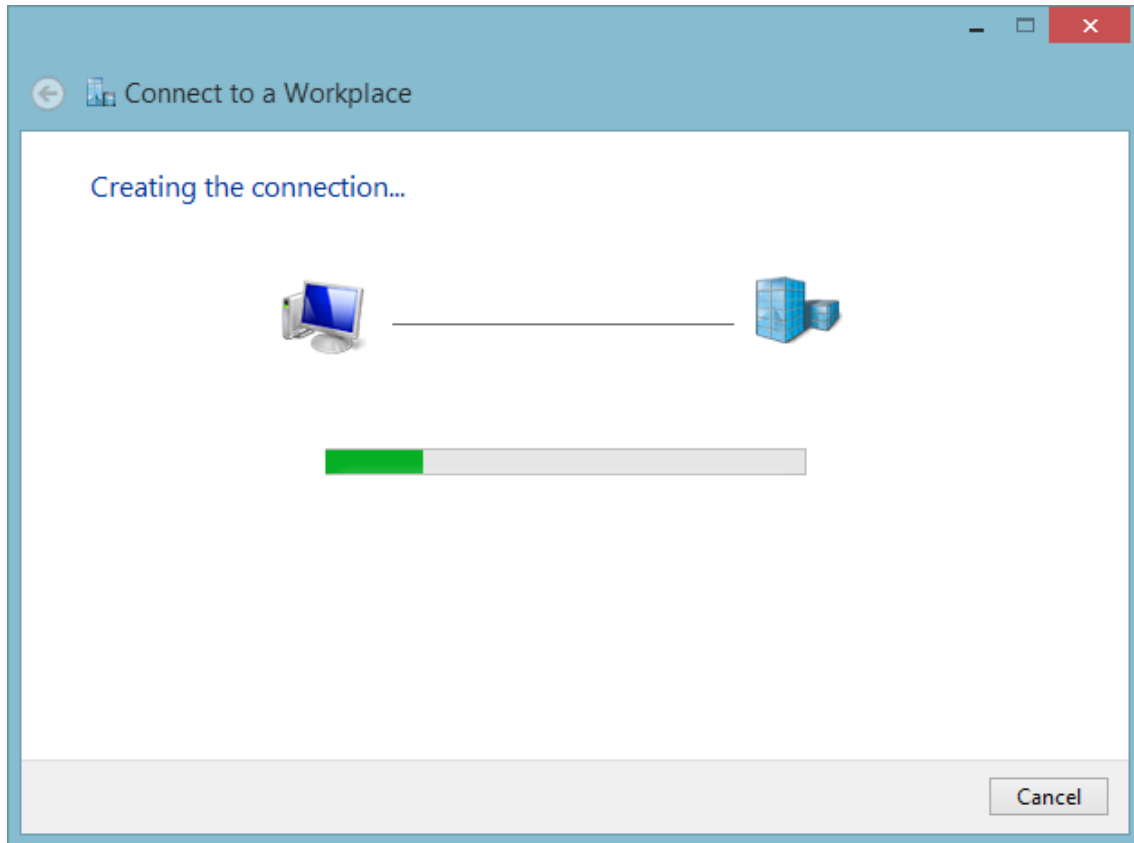
☒ Use a smart card

☐ Remember my credentials

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Create Cancel

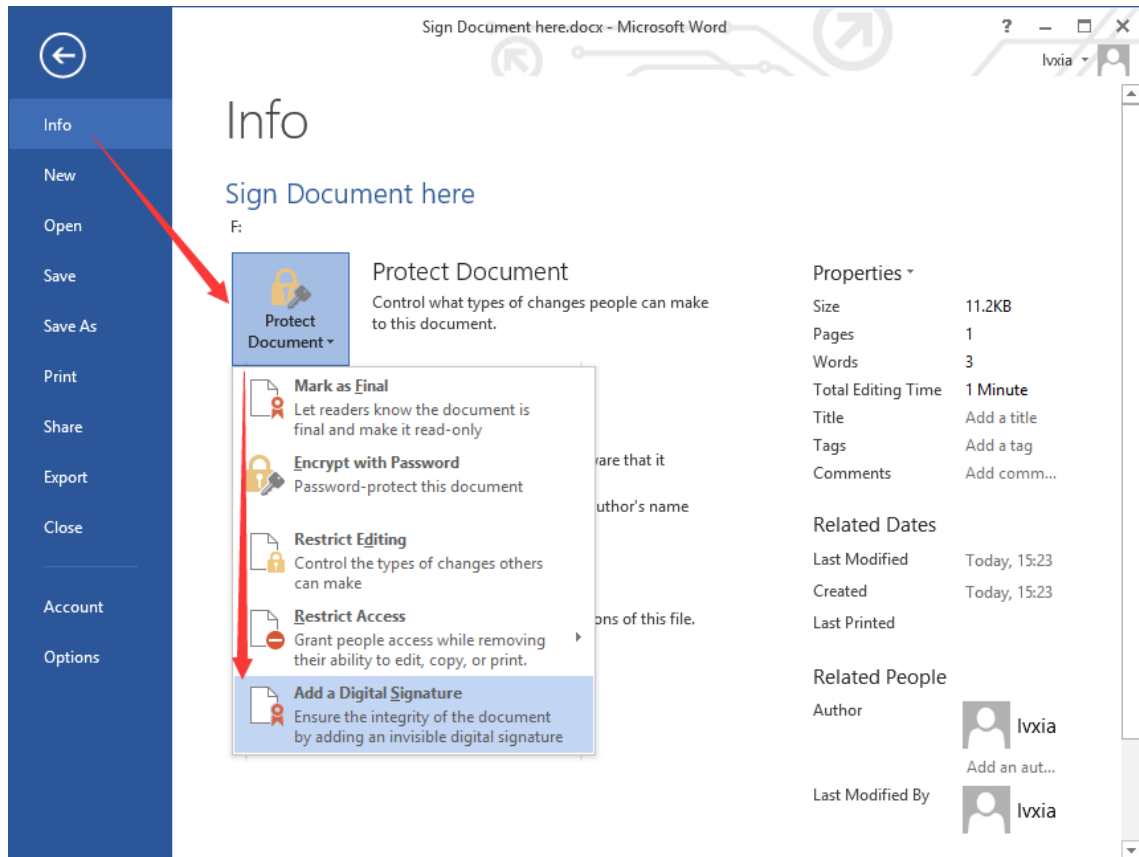
6. Now your VPN connection has established



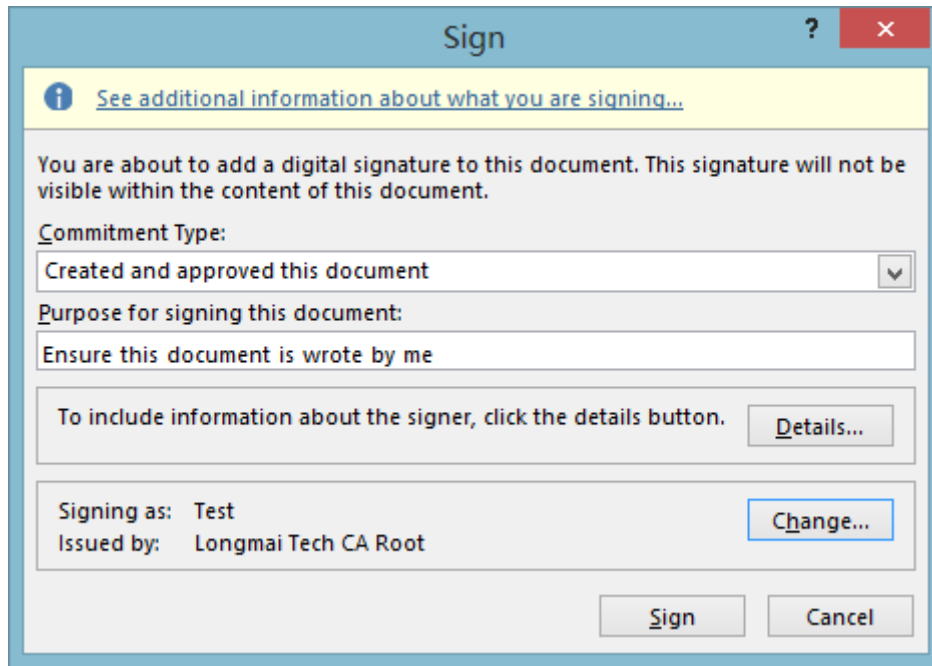
Chapter 4. Office Document Signature

1. Sign office document

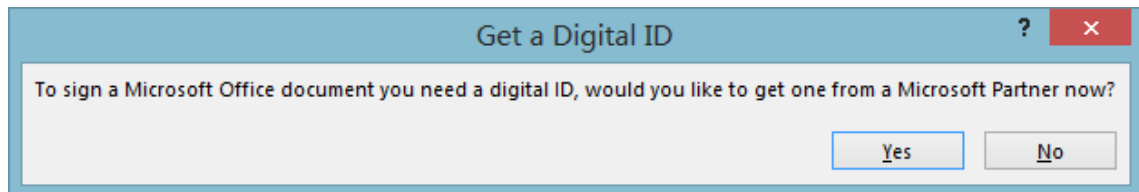
1. Ensure mToken CryptoID contains required certificate. Connect mToken CryptoID to the PC.
2. In office word document, select **File** → **Info** → **Add a Digital Signature**



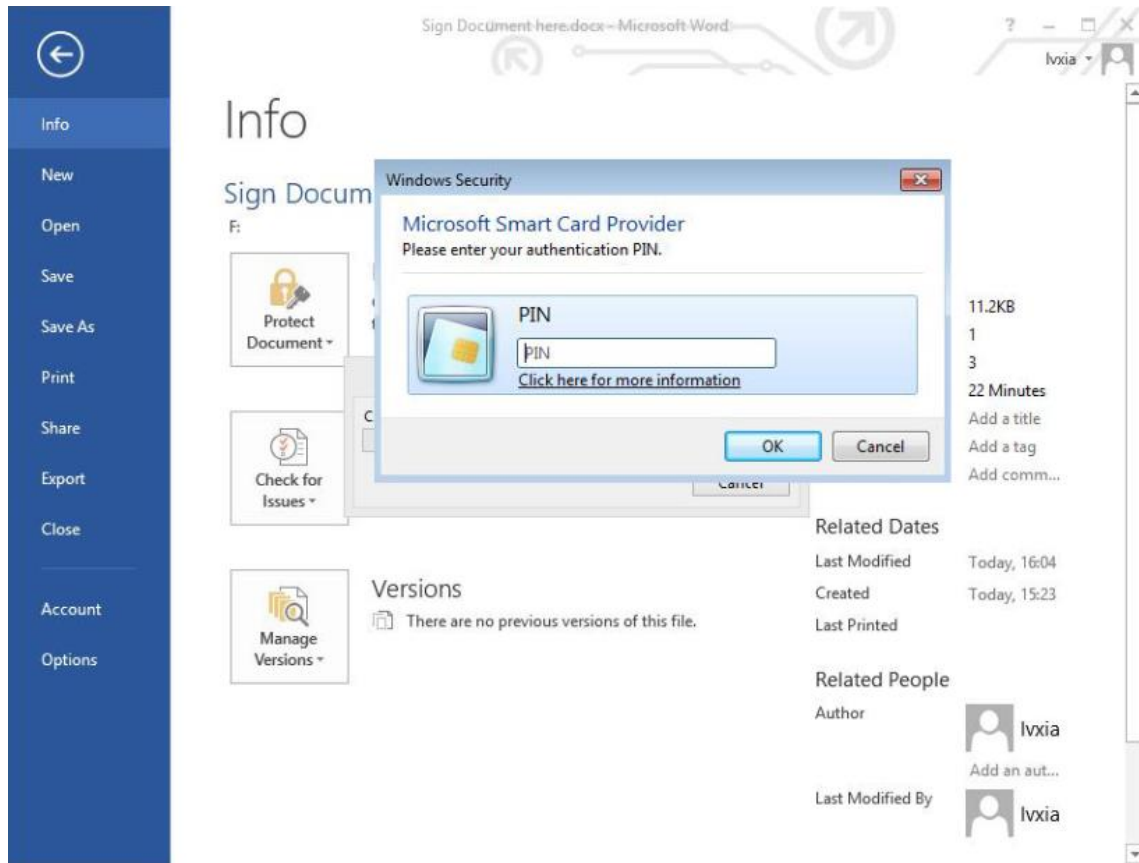
3. Select **Commitment Type** and write your **Purpose**. By default, the latest certificate will be selected, but you can also click **Change** to select your preferred signature certificate.



4. If you don't see the window above, but instead receive below pop-up window. It means there is no certificate found on your computer; please make sure the connected mToken CryptoID contains corrected certificate. If you can see the window above, please **Sign** and skip this step.



5. Then click **Sign**, you will be asked to input device User PIN.
Default User PIN is: 12345678 (If you changed it, please use your new user pin)

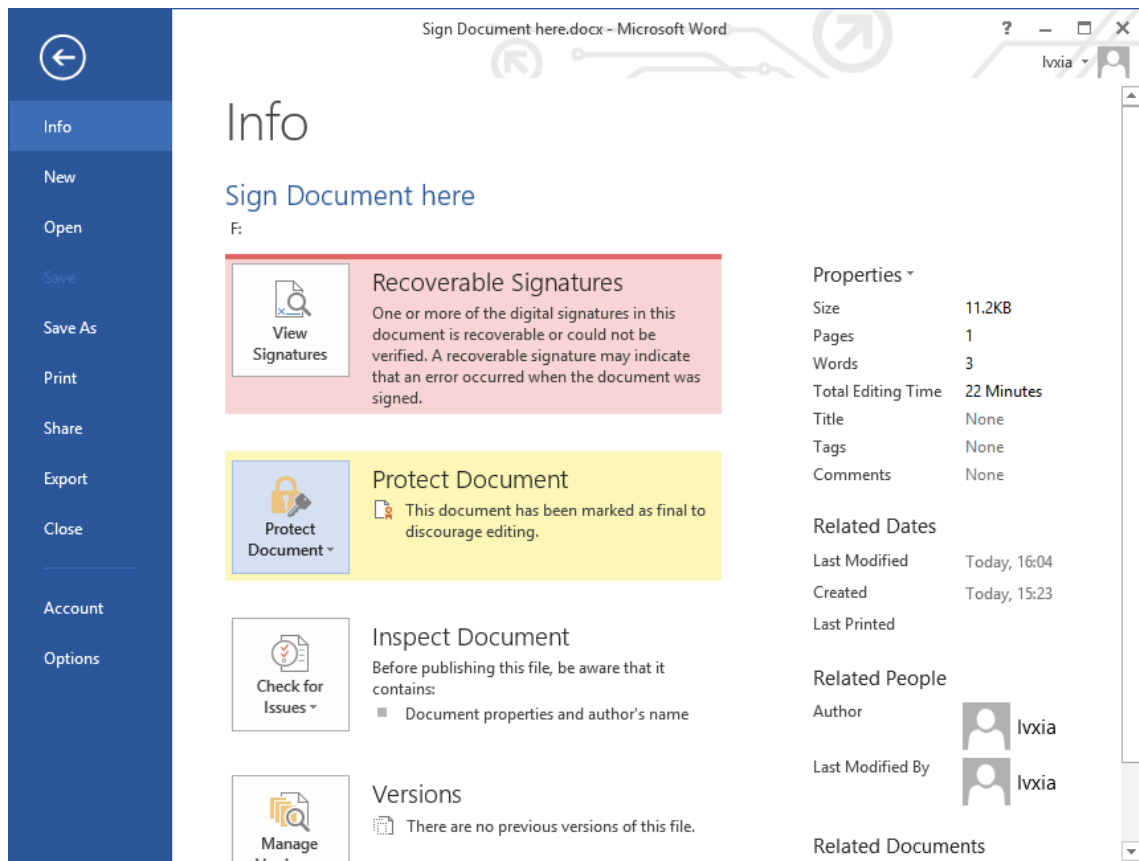


6. Click **OK** to sign this document; you will get a success confirmation dialog.

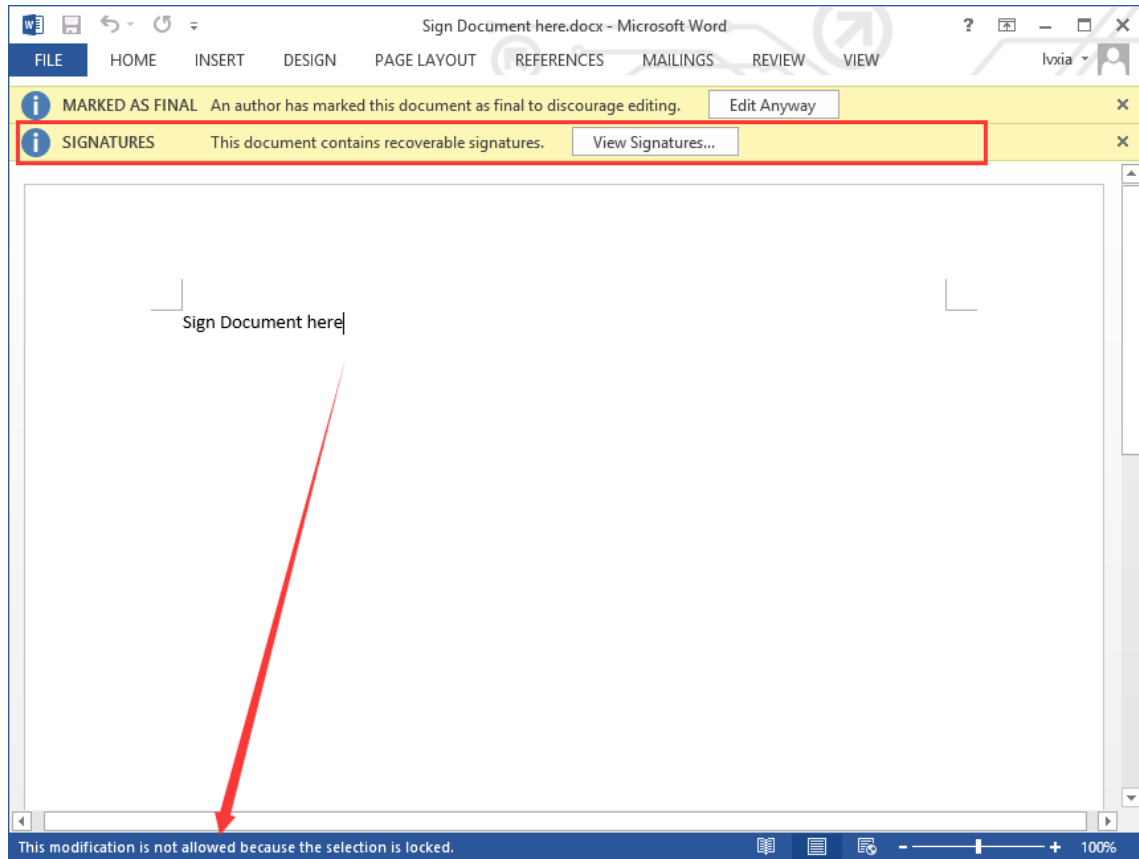


7. Click **OK**. (you will find that the document has been signed)

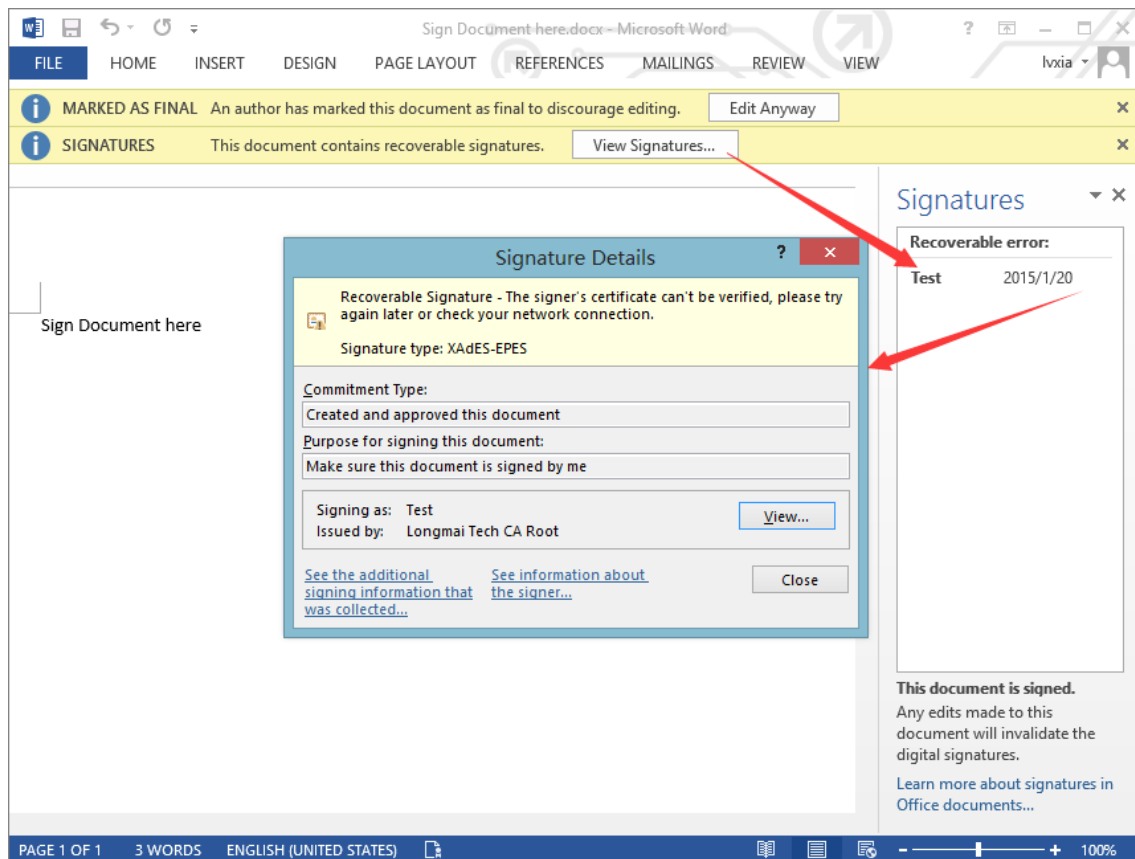
C



8. For example, when I try opening this document and attempt to modifying it, the message about document is locked is displayed, and modifying it needs token verification. Meanwhile, the information we have shown us that this document is signed.



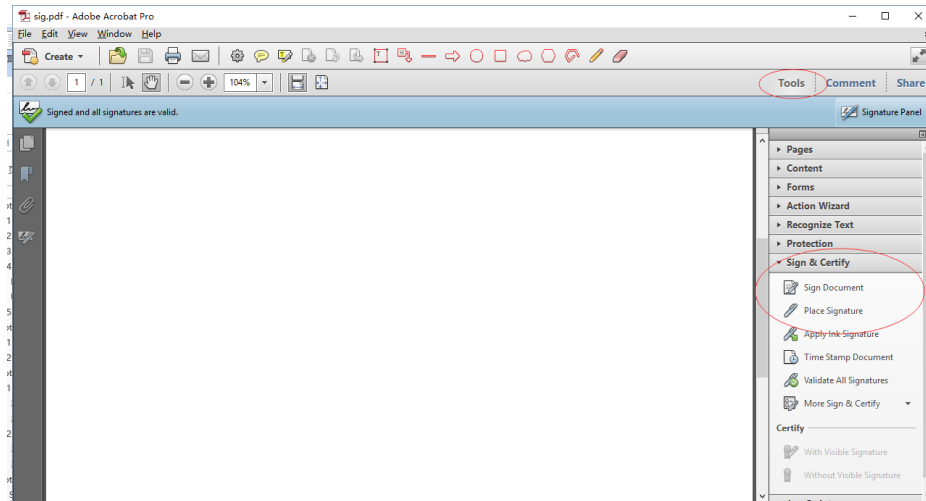
9. Click **View Signatures**, select certificate to view details.



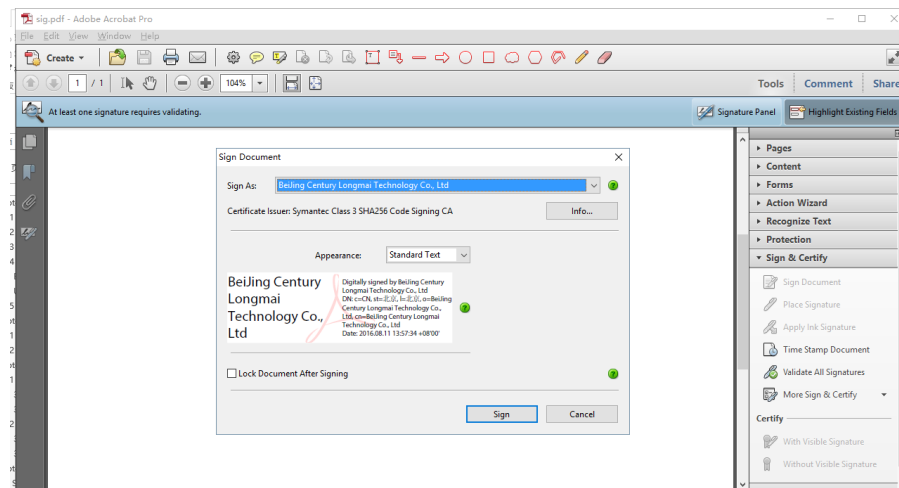
Chapter 5. Adobe Acrobat Pro Signature

The Adobe Acrobat Pro supports digital signature, the Adobe Acrobat Reader only could be used for signature verification. To sign the PDF file:

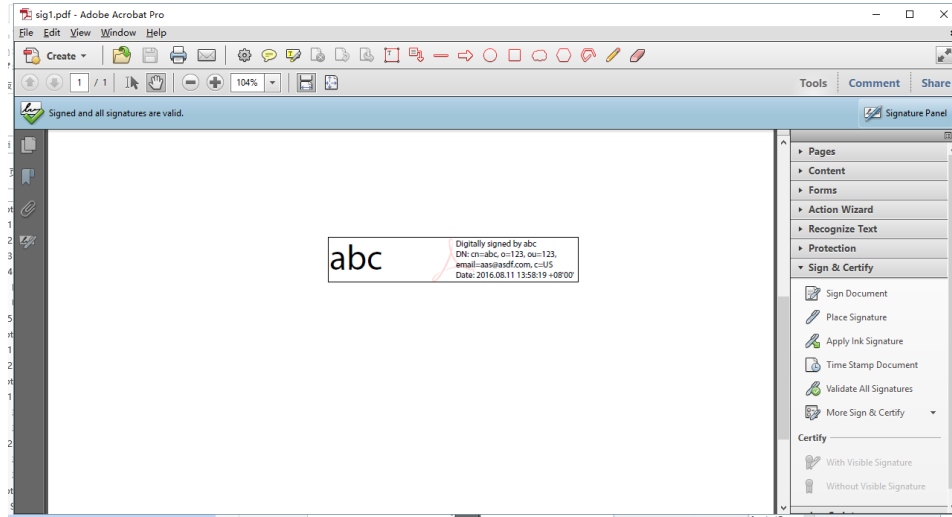
1. Turn on the Tools panel and select “Sign Document” or “Place Signature”:



2. The certificate dialog will pop up and select the certificate from the list:



3. Click “sign” button to finish the digital signature and save into pdf file.



4. Then you can open the file with a PDF reader to check the signature. For example:

